BIRMINGHAM CITY University

Integration of Cybersecurity in BIM-enabled Facilities Management Organisations

A thesis by:

Nikdokht Ghadiminia

Submitted in fulfilment of the requirements of the degree of

Doctor of Philosophy

Faculty of Computing, Engineering and Built Environment (CEBE)

Birmingham City University

May 2021

Acknowledgements

I would like to express my sincere gratitude to my director of studies and main supervisor, Dr Mohammad Mayouf, for his guidance and insight, as well as his endless support throughout my PhD journey. Thank you for your incredible patience, understanding and encouraging words when the path was not smooth. I am grateful for your constructive comments, which was never a let-down, but always a step forward. And thank you for the positive words, at the end of each conversation and every meeting, which kept me going.

I am sincerely thankful to my assessors, Professor Mark Shelbourne, and Professor Mohamad Kassem, for their invaluable feedback, and precious insight, on my thesis. I am honoured to have the opportunity of meeting with two outstanding minds, and exemplary characters, from which I have learned plenty.

I am especially grateful to Professor Peter Larkham, whose support has helped me to get through the course of my PhD. I am also thankful to my annual review panellists, Professor Franco Cheung and Dr Hong Xiao, whose critical feedback led to substantial improvements in my work. This journey would have been more difficult, without Sue Witton and Andrea Mondokova, whose kind help has always served as a blessing.

My special thanks go to Professor Hanifa Shah, who listened, understood, and believed in me. I am forever thankful for your support, without which, this research would have not been made possible. You are a true representation of modesty, respect, and wisdom.

I am sincerely grateful to my MSc supervisor, Professor David Walker, who believed in me, and inspired me towards achieving the best. Words cannot express my appreciation for your kind heart, great soul, and precious advice, throughout all these years.

And at last, but not the least, to Birmingham City University colleagues and friends, and the participants of this research, thank you all.

“If it is to be, it is up to me.”

- William H. Johnsen

Abstract

Building Information Modelling (BIM) enables the creation, exchange and storage of digital information which represents digital and physical assets within a facility. The data within the in-use phase of a BIM project life cycle incorporates the highest level of details, where the as-built data of the facilities are managed and maintained by the facilities management (FM) organisations. The connection of BIM with the FM systems facilitates access to as-built and as-maintained data of all components within a facility, which may enable control of the devices and systems within the facility. Hence, facilities and their occupants become ever more vulnerable to cyber-attacks with malicious intentions of harming the occupants or disrupting and destructing the facilities. Thus, effective cybersecurity management is required to protect data.

Findings from the review of literature were summarised in a cybersecurity risk matrix, to bridge the concepts of cybersecurity and BIM in FM by unveiling the impact of a cybersecurity attack, resulting in a compromise of the integrity, availability, and confidentiality of data in various task areas of a BIM-enabled FM (BIM-FM) organisation. Hence, emphasising the significance of effective and efficient management of cybersecurity in preserving the benefits associated with the implementation of BIM in FM. Review of the literature showed that both academia and industry are more focused on the technical aspects of using BIM in FM, which is often coupled with an overdependency on technical cybersecurity measures. Thus, investing in a mature implementation of BIM, that includes cybersecurity considerations from a people and process perspective, is often overlooked in FM organisations. This has resulted in an increased vulnerability to a cybersecurity attack that may compromise the potential BIM benefits in FM. Therefore, this study sought to shift focus to the people and process aspects of the issue of cybersecurity in BIM-enabled FM, by exploring the people and process related BIM and cybersecurity determinants that contribute to a more cybersecure BIM-FM.

An inductive approach to the research facilitated a multi-disciplinary exploration of the concepts of BIM and cybersecurity, which resulted in the demarcation of the research focus to the BIM enabled facilities management organisations. This was followed by a literature review and qualitative analysis of secondary data from BIM maturity models and cybersecurity best practice guidelines to investigate the requirements of a cybersecure implementation of BIM in FM. Findings were structured to form the primary research framework, that was further enhanced and improved using the empirical findings collected via 25 semi-structured

interviews with facilities management professionals. Findings from the thematic analysis of the interviews were coalesced with the literature review findings to develop the BIMCS-FM framework upon the primary research framework. The BIMCS-FM framework presents the determinants of a cybersecure BIM in FM and their interconnections, to assist BIM-FM organisations in their approach to cybersecurity management. The framework was validated using expert opinion that was carried out using semi-structured questionnaire, that was qualitatively analysed to make final revisions on the framework.

The BIMCS-FM framework acts as a prompting mechanism for BIM-FM organisations to integrate cybersecurity within all aspects of BIM in FM. This framework expands the scope of BIM maturity, by incorporating cybersecurity considerations as part of the management of BIM in FM. Hence, creating a unified approach towards the management of both BIM and cybersecurity in FM. The application of this framework to BIM-FM can benefit from the future development of process models to enable the build-up of knowledge, skill sets, awareness and culture that is required for a cybersecure implementation of BIM. This study also provides a foundation for future research into the complexities of cybersecurity in protecting the digital information in various task areas of a BIM-FM organisation.

Table of Contents

Dedication i

Acknowledgements ii

Abstract iv

Table of Contents vi

List of Tables xi

List of Figures xi

1 Chapter One: Introduction 1

1.1 Introduction 1

1.2 Research Background 1

1.3 Research Problem 2

1.4 Research Aims and Objectives 4

1.5 Research Question 4

1.6 Thesis Outline 4

2 Chapter Two: Literature Review 7

2.1 Introduction 7

2.2 BIM: A Critical Review 7

2.2.1 Definitions of BIM 7

2.2.2 Levels of BIM Adoption 8

2.2.3 Digital Collaboration in BIM 10

2.2.4 BIM Lifecycle 13

2.2.5 BIM Data Across Project Phases 14

2.2.6 Cybersecurity across BIM Lifecycle 17

2.3 Role of BIM in Facilities Management 20

2.3.1 Overview of Facilities Management 20

2.3.2 BIM-Enabled Facilities Management (BIM-FM) 21
2.3.3 BIM Challenges in FM 27
2.4 Cybersecurity Concept in Digital Built Environment 30
2.4.1 Cybersecurity Threats 31
2.4.2 Cybersecurity Risks 33
2.4.3 Risk Matrix: Cybersecurity Risks for BIM-enabled FM 35
2.4.4 Cybersecurity of BIM-enabled Facilities Management 38
2.5 Cybersecure management of BIM in FM 40
2.5.1 BIM Maturity Models 40
2.5.2 Cybersecurity Considerations in BIM-FM 52
2.6 Primary Research Framework 62
2.7 Conclusion 64
3 Chapter Three: Methodology 66
3.1 Introduction 66
3.2 Research Philosophy 66
3.2.1 Critical Realism 67
3.3 Methodology in Critical Realism 68
3.4 Research Approach 69
3.5 Research design 70
3.6 Qualitative Research Methods 72
3.6.1 Preliminary Explorations- Review of Literature 73
3.6.2 Secondary Data Analysis 73
3.6.3 Primary data collection- Interviews 75
3.6.4 Thematic Analysis of Data 79
3.6.5 Framework Validation: Expert's Review 80
3.7 Research Quality 82
3.7.1 Reliability and Trustworthiness 83

3.8 Ethical considerations 84
3.8.1 Confidentiality & Anonymity 85
3.8.2 Level of Sensitivity 85
3.9 Conclusion 86
4 Chapter Four: Empirical Findings- Interviews 87
4.1 Introduction 87
4.2 Qualitative Data Analysis 87
4.2.1 Setup and Coding 87
4.2.2 Focus of interview questions 88
4.3 Thematic analysis results 89
4.3.1 General views of respondents on BIM and Cybersecurity 90
4.3.2 Theme One: BIM-FM determinants 93
4.3.3 Theme Two: Cybersecurity Determinants 107
4.3.4 Theme Three: Challenges of CS Integration in BIM-FM 119
4.4 Conclusion 127
5 Chapter Five: Discussion 129
5.1 Introduction 129
5.2 Assimilation of findings 129
5.2.1 Strategic Integration of Cybersecurity in BIM-FM 130
5.2.2 Implementational Integration of Cybersecurity in BIM-FM 137
5.2.3 Integration of cybersecurity in BIM-FM Performance 143
5.3 Framework Development 147
5.3.1 Strategy layer 148
5.3.2 Performance layer 149
5.3.3 Implementation layer 150
5.3.4 Enhancing the scope of BIM maturity 151
5.3.5 BIM-FM Cybersecurity Considerations 152

5.3.6 BIMCS-FM Framework....153
5.4 Conclusion....156
6 Chapter Six: Validation of the research framework....157
6.1 Introduction....157
6.2 Validation Using Expert Review....157
6.3 Questionnaire Design....160
6.4 Validation....160
6.4.1 Applicability of the three layers of strategy, implementation, and performance 161
6.4.2 Applicability of the determinants of cybersecurity integration in BIM-FM....161
6.4.3 Validation of the interconnections of the layers within the framework....164
6.4.4 Understanding of concepts and their interconnections within the framework by facilities management organisations....166
6.4.5 Value of the framework for BIM-FM organisations....167
6.5 Revision to Framework....167
6.6 Framework Beneficiaries....170
6.7 Conclusion....172
7 Chapter Seven: Conclusion....173
7.1 Introduction....173
7.2 Results attribution to research objectives....173
7.2.1 Research Objective I –To critically explore the cybersecurity risks in various phases of a BIM lifecycle....174
7.2.2 Research Objective II- To identify the risk factors affecting cybersecurity in BIM-FM organisations....174
7.2.3 Research objective III- To determine the requirements of a cybersecure implementation of BIM in FM....175
7.2.4 Research objective IV. To develop and validate a framework that supports an improved integration of cybersecurity considerations in BIM-FM organisations....176

7.3 Contributions 176
7.3.1 Theoretical Contributions 177
7.3.2 Contributions to Practice 177
7.4 Limitations 179
7.5 Future Studies 180
7.6 Final Thoughts 181
List of References 182
Publications 226
Appendix 1. Interview Participation Form 228
Appendix 2. Validation Questionnaire Consent Form 230
Appendix 3. Interview Questions 232
Appendix 4. Validation Questionnaire 235

List of Tables

Table 1-BIM benefits in FM 26
Table 2- BIM-FM Cybersecurity Risk Impact 37
Table 3- BIM Maturity Models Evaluation Focus 45
Table 4- Participants' Roles & Organisational Sector 78
Table 5- Participant's Roles & Organisational Sector 81
Table 6-Strategy Layer Themes and Sub-themes 130
Table 7-Implementation Layer Themes and Sub-themes 138
Table 8-Performance Layer Themes and Sub-themes 144
Table 9- Validated BIMCS-FM Determinants' Description 169
Table 10- Interview Questions 232
Table 11- Validation Responses 235

List of Figures

Figure 1- Identification of the research problem 3
Figure 2- Thesis Outline 6
Figure 3- BIM Levels, Source: bimportal.scottishfuturetrust.org.uk 10
Figure 4- BIM Phases, Resource: Succar, (2009) 13
Figure 5- Conceptual Cybersecurity Risk in a BIM Project (Whole Lifecycle) 19
Figure 6- Synergy of Identified Determinants for a Cybersecure BIM-FM 63
Figure 7- Primary Research Framework 64
Figure 8-Critical Realism View (Mingers, 2004) 67
Figure 9-Inductive Research Process (Trochim and Donnelly, 2001) 69
Figure 10- Research Design 72
Figure 11- Multi-disciplinary analysis of secondary data for identification of determinants 74
Figure 12- Data Analysis Process 87
Figure 13- Interview Themes & Sub-themes 89
Figure 14-BIMCS-FM Research Framework 154
Figure 15- Validated BIMCS-FM Framework 169

Chapter One: Introduction

1.1 Introduction

This chapter introduces this research study, by presenting an overview of the research scope and providing a background of the key domains including building information modelling (BIM), BIM-enabled facilities management (BIM-FM) and cybersecurity management within the built environment. The chapter proceeds by discussing the research rationale and illustrating the research aim, research question and objectives. Finally, the chapter will conclude by discussing the outline of the thesis.

1.2 Research Background

The Architectural Engineering Construction and Operations (AECO) industry has opted for the adoption of technology and digital tools across all its sectors (Azhar, 2008). Many studies have emphasised the need for the employment of digital technologies, such as Building Information Modelling (BIM), for optimising processes and increasing efficiency across the whole life cycle of a construction project (Bughin *et al.*, 2017). BIM facilitates a collaborative approach towards the generation, utilisation and management of digital information and BIM models of a physical asset, and its attributed operational characteristics (Ghaffarianhoseini *et al.*, 2017a).

Although the benefits of BIM are well demonstrated within all phases of a project lifecycle, it is particularly beneficial in optimising efficiency during the in-use phase of the project (Edirisinghe *et al.*, 2017). The operations and maintenance work in this phase are collaborative in nature. Facilities management (FM) organisations liaise with contractors, sub-contractors, suppliers and clients/owners for various projects (Abdullah *et al.*, 2013). All stakeholders commonly communicate through a digital common data environment (CDE) for an enhanced collaboration which encapsulates voluminous virtual information linked with the physical attributes of a building/facility (Louis and Dunston, 2018).

Maglaras *et al.*, (2018), also state that the rapid growth of connectivity between the facilities management systems and the real-time monitoring capabilities enabled by BIM, have increased the risk of a cybersecurity attack. However, this is overlooked in favour of the numerous advantages that technologies bring to the industry (Boyes, 2015a). Cybersecurity threats that can potentially disrupt the functionality of facilities, compromise the physical security of the occupants and incur financial losses for businesses (Boyes, 2015b). A cyber-security breach

within a BIM-enabled facilities management allows unauthorised access to the building management systems and real-time information for all aspects of the built facility (Mutis and Paramashivam, 2019). This results in significant risks to the health and safety of the occupants and the functionality of the facility/building, as well as the financial and reputational aptitudes of the stakeholders (Nazir *et al.*, 2017; Purpura, 2019). Therefore, it can be concluded that although a cybersecurity attack can have adverse effects on all phases of a BIM project lifecycle, its implications within the in-use phase, managed and maintained by facilities management is most critical.

Traditionally, IT or technical experts were seldom held responsible for the management and monitoring of information security (Tuptuk and Hailes, 2018). However, an isolated approach as such is criticised in the literature for its inefficiency and ineffectiveness in managing cyber security within digital organisations, such as BIM-FM organisations (Von Solms and Van Niekerk, 2013). The transition of the FM organisations from traditional to BIM-enabled ways of working, challenges the achievement of a mature implementation of BIM (Pärn *et al.*, 2017), which can act as a cybersecurity vulnerability with the accompanying cybersecurity threats to FM organisations. Therefore, cybersecurity should also be considered within both the people and the process aspects of BIM-FM implementations.

For a holistic approach to the management of cybersecurity, a number of studies have proposed organisational cyber-security management within the context of the enterprise risk-management domain (ERM), where risk is assessed through a multi-perspective lens (Min *et al.*, 2015). Researchers have historically identified the need for strategic planning to embrace enterprise risk management which takes into account cybersecurity risks within digitalised organisations (Siponen and Willison, 2009). This is applicable to BIM- enabled facilities management organisations seeking to enhance their cybersecurity management capabilities, by a seamless integration of cybersecurity considerations within all aspects of implementing BIM in FM. Through the assimilation of BIM and cybersecurity capabilities, this integration will result in an improved state of cybersecurity within BIM-FM organisations (Boyes, 2015a; Mantha and de Soto, 2019).

1.3 Research Problem

A multi-disciplinary exploration of the concepts of BIM and cybersecurity demonstrated the adverse implications of a cybersecurity attack within the in-use phase of a BIM project lifecycle (Boyes, 2015a; Maglaras *et al.*, 2018). The literature illustrated that the impact of a

cybersecurity attack in this phase can extend to loss of life and injury for the facilities' residents, as well as significant financial and reputational losses for the organisations involved in the management and maintenance of these facilities (Boyes, 2015c; Pärn *et al.*, 2017). Further review of literature in BIM enabled facilities management shed the light on the benefits of implementing BIM in FM. These benefits were mainly dependent on the availability of accuracy of the right information at the right time. As the facilities management organisations are still transitioning from the traditional ways of working to BIM enabled facilities management, they face a number of challenges and shortfalls in the adoption of BIM, that limit the accomplishment of the full potentials of BIM in FM.

Incorporating knowledge from the review of literature in cybersecurity, it was identified that challenges of BIM in FM act as a cybersecurity vulnerability, that may be exploited by malicious cybersecurity threats (Figure 1). Successful exploitation of these vulnerabilities may compromise the BIM benefits in FM, through manipulation of the availability, integrity, and confidentiality of information.

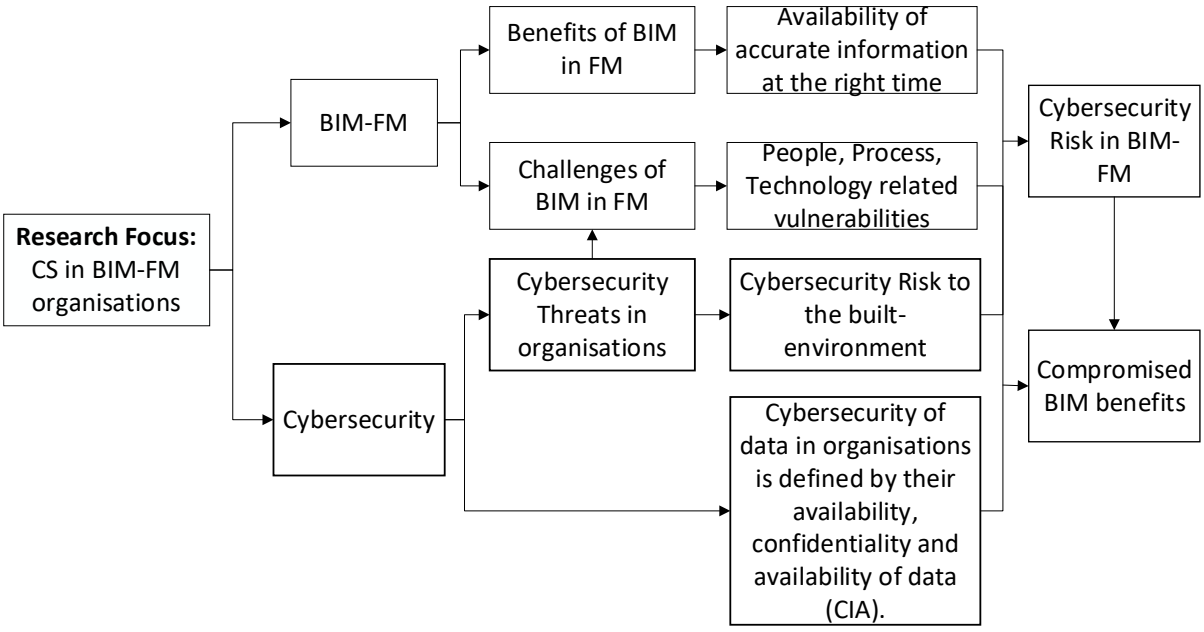


Figure 1- Identification of the research problem

Hence, having an effective approach to the management of cybersecurity within BIM-FM organisations is essential. However, the acknowledgement of the cybersecurity risk and the poor cybersecurity status in BIM-FM is limited (Mantha & Karri, 2020; Mayo and Snider, 2016). With reference to this and recognising that cybersecurity-related research for BIM

within the built environment is still developing, the focus leans towards improving the technical and modelling capabilities of BIM. Although this support overcoming the technological challenges encountered in the implementation of BIM, it lacks acknowledging the people and process sides, which contribute towards an increased risk of a cybersecurity attack via the exploitation of the resulting vulnerabilities. Therefore, there is a need to acknowledge the cybersecurity vulnerabilities and risks associated with the implementation of BIM in FM, and plan for a robust management of cybersecurity, that includes people, process, and technology. This will enable a unified management of BIM and cybersecurity, which supports an informed consideration of cybersecurity related issues and complexities in BIM-FM organisations.

1.4 Research Aims and Objectives

The research aim is to develop a framework that assists the incorporation of cybersecurity considerations BIM-enabled facilities management organisations. To support the accomplishment of the aim, and identify how can the management of cybersecurity improve in BIM-FM organisations, the following objectives were defined and fulfilled:

I. To critically explore the risks of cybersecurity across all phases of a BIM project lifecycle.
II. To identify the risk factors affecting cybersecurity in BIM-FM organisations.
III. To determine the requirements of a cybersecure implementation of BIM in BIM-enabled facilities management organisations.
IV. To develop and validate a framework that supports an improved integration of cybersecurity considerations in BIM-enabled facilities management organisations.

1.5 Research Question

Following the preliminary explorations of the research scope, the research question was developed as:

-What are the key factors that contribute to the integration of cybersecurity considerations within BIM enabled facilities management organisations?

1.6 Thesis Outline

This thesis aims to articulate the exploration and investigation of the ways in which facilities management organisations can improve their cybersecurity in the implementation of BIM. In

doing so, this chapter provides an introduction to the research (See Figure 1). The second chapter is an in-depth exploration of BIM, BIM-enabled FM, and cybersecurity in the built environment, which highlights the criticality of cybersecurity in facilities management organisations, as part of the overall BIM life cycle. This is followed by further investigation into the issue of cybersecurity associated with the challenges of BIM implementation in FM. Exploring the theory and practice of cybersecurity management in BIM-FM organisations directs the focus of the research to the people and process aspects of BIM. Therefore, a thematic exploration of the people and process determinants of a cybersecure BIM in FM is conducted, upon which the initial research framework was developed (Chapter 2). The third chapter is a road map of the research which presents a detailed explanation of the research approach, philosophical positioning, methodology and most importantly, research quality and ethical considerations.

Chapter four reports on findings from the semi-structured interviews conducted to further expand and validate the initial research framework. Hence, Chapter five discusses the empirical findings in relation to the theoretical findings, to restructure and expand the primary research framework. Chapter six describes the validation of the framework using expert review. Finally, chapter seven presents the attribution of findings with the research aim, research question and objectives and discusses the limitations of the work, along with the contributions to the industry and academia.

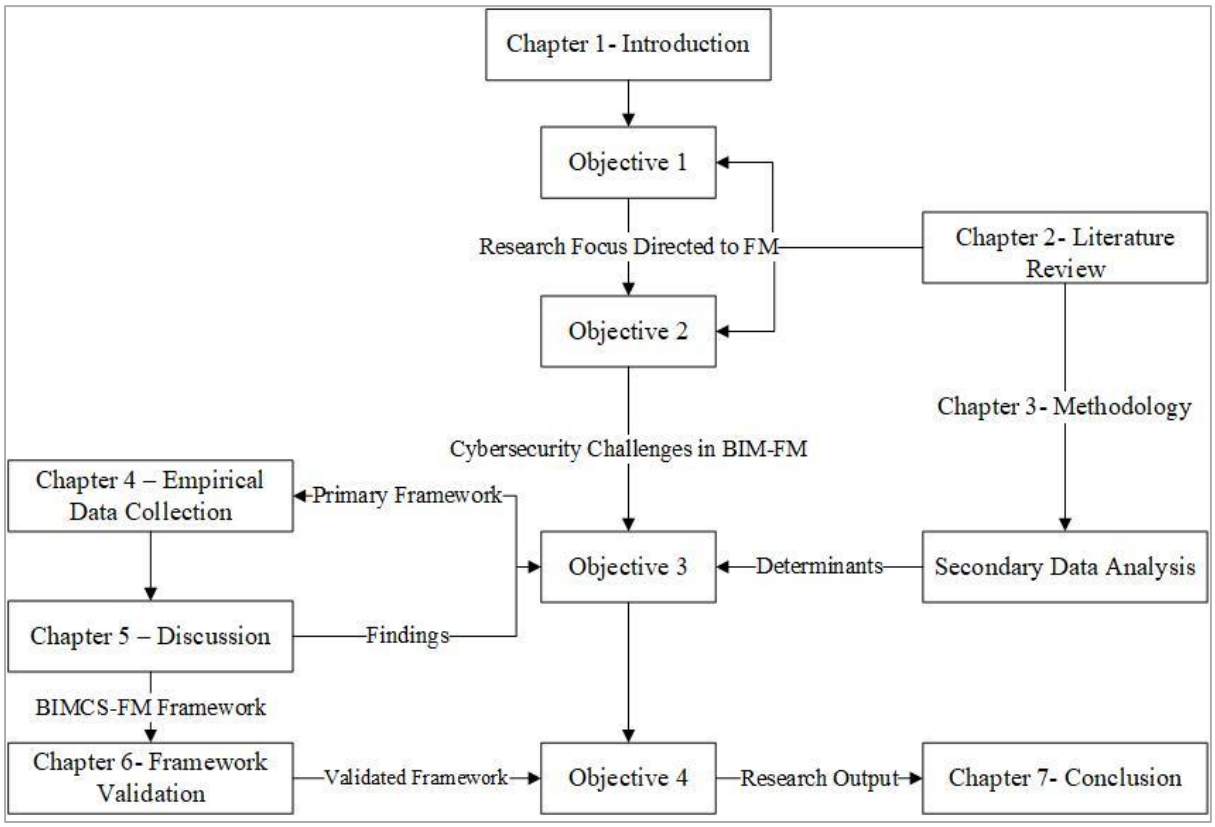


Figure 2- Thesis Outline

Chapter Two: Literature Review

2.1 Introduction

This chapter aims to provide an overview of the three domains of Building Information Modelling (BIM), facilities management and cybersecurity within the built environment, to highlight the criticality of the issue of cybersecurity in the in-use phase, and in particular, BIM-FM organisations, as part of the overall BIM lifecycle. The review of BIM and cybersecurity directs the focus of the research to the cybersecurity of BIM-enabled facilities management organisations (BIM-FM), following which the cybersecurity implications, and the underpinnings of cybersecurity vulnerabilities and challenges within the BIM-enabled FM organisations is reviewed. The chapter also provides a conceptual risk matrix that brings the three concepts of cybersecurity, BIM, and FM together. This chapter will look further into the requirements of a cybersecure BIM in FM. In doing so, an analysis of secondary data within the literature is conducted to identify the determinants of a cybersecure BIM-FM. The chapter concludes with a diagram of the theoretical framework of the research that portrays the integration of cybersecurity considerations in strategic, implementation and performance aspects of a BIM-enabled FM organisation.

2.2 BIM: A Critical Review

The architecture, engineering, construction and operations (AECO) industry has always sought optimisation of processes and procedures for increasing efficiency within projects (Azhar et al., 2008). In 2011, the UK government mandated the use of Building Information Modelling (BIM) in all public sector construction projects to enable digitisation of processes, resulting in optimised project management and execution as well as an enhanced efficiency throughout all stages of a project lifecycle (Ghaffarianhoseini *et al.*, 2017a).

2.2.1 Definitions of BIM

The literature shows that there are multiple definitions for the term Building Information Modelling (BIM). Some research studies have claimed that BIM stands for building information management or building information modelling and management (RIBA, 2012). BIM could be defined differently based on the background and experience of experts working within a BIM-enabled project (Khosrowshahi and Arayici, 2012; Sacks *et al.*, 2018; and Hardin, 2009). The definition of BIM was presented in some research studies as a tool that can be used for simulating the construction and/or operational processes of a facility, from which

the resulting model would be an accurate representation for the physical components and their interactions with one another (Morlhon *et al.*, 2015). In defining BIM, some research studies considered BIM as a three-dimensional computational tool (Ellis, 2006). However, others considered it as an interactive tool for information modelling and management, rather than object-oriented software (Tang *et al.*, 2020). In another definition by Schade, (2011), BIM is defined as a process that supports communication, collaboration, simulation and optimisation. The definition of Gu *et al.*, (2008), suggested that BIM is a digital representation of the information of a facility throughout the different phases of the project lifecycle using a structured-data repository. This is in agreement with the definition of Smith and Figp, (2010) definition in which BIM was assumed as a structured set of data that can easily be shared amongst all stakeholders. BIM can also be defined in the context of information management in which the information is managed throughout the lifecycle of the project, starting with the design process, through the construction and finally into the in-use phase of the facility (Ghaffarianhoseini *et al.*, 2017a). Smith and Figp (2010) also suggested that BIM is an image digitisation technology from which users can determine service costs inside buildings. A comprehensive definition of BIM is provided by Ahmad *et al.*, (2012), stating that BIM is a powerful tool that enables information sharing, modelling, design evaluation, stakeholders collaboration and management of models throughout the lifecycle of a project. As highlighted by NBIMS Committee (2007), Ahmad (2012) and State of Ohio (2010), there are three main aspects to BIM:

• A product which is considered as a structured database used in representing, simulating and automation of buildings.

• An activity of developing a building information model in which processes are being created, scheduled, and organised.

• A system for increasing the quality and efficiency of communication inside organisations by maintaining and sharing real time information.

2.2.2 Levels of BIM Adoption

The transformation of the AECO industry from the traditional ways of working to a BIM-enabled modus operandi has led to the introduction of four levels of BIM adoption (Levels 0,1,2,3,4) throughout the lifecycle of a BIM project (BIM United, 2020). As shown in figure 4, each level entails pre-set milestones that can be achieved through technological excellence and improving upon the collaborative methods used amongst the stakeholders. Prior to the first

level, level 0 indicates that there is no collaboration, and the project is based on 2D CAD drawings. In this level, paper and print outs of documents are the main data that are used in the project. Because level 0 is obsolete nowadays, in Level 1, BIM project commences by drafting 3D drawings. 3D drawings are used during the concept phase, whereas 2D is usually used in acquiring approvals for design and documents. The communication and data exchange for stakeholders takes place using a Common Data Environment (CDE). A CDE is considered as a platform used for gathering, managing, and exchanging graphical and non-graphical information, to enable all project stakeholders to access the project related information (RICS, 2017). Using common data environments such as SharePoint, Viewpoint, One Drive, Autodesk 360 (Radl and Kaiser, 2019) in BIM projects enable easier access to the required information which saves time and effort for finding relevant information for a component, structure or asset (Boxall, 2015). Although collaboration is limited at this level, British Standards (e.g. BS 1192:2007) are used to regulate data-sharing processes within collaborative projects (BIM United, 2020). There are several requirements in order to achieve level 1. For instance, roles should be clearly defined as mentioned in the CIC BIM Protocol (CIC, 2013). In this regards, Delany (2019) points out that compliance to standards relevant to BIM-enabled projects is also another consideration for BIM level 1 projects.

Level 2 allows better coordination and easier access to the project BIM model and digital information for all team members and stakeholders (BIM United, 2020). Employing digital information sharing processes is a fundamental requirement for deploying level 2 BIM. In a BIM-enabled project, team members would often be working on different files; and data would be shared automatically using data-exchange file format. In this way, organisations would be able to merge data from external sources with their local models and create the BIM model. This requires facilitation and installation of software that support common file formats (Leite *et al.*, 2011; Richard, 2018).

The UK government has mandated the use of BIM level 2 for all public projects, however level 3 BIM is proposed to bring new horizons to the industry. At this level, all stakeholders collaborate on a centralised model that contains all information of a facility in real time (Gu and London, 2010; Richard, 2018). In this level, international 'Open Data' standards are required to enable data sharing across the industry and promote consistency of work processes and result in optimum collaboration (Gu and London, 2010). Additionally, the requirements of a level 3 BIM encompasses training and upskilling considerations for the public-sector organisations to achieve the full benefits of BIM within their projects (Richard, 2018).

Most organisations are still working to improve their digital collaboration processes to fulfil all requirements of level 2 and level 3 BIM in their organisations. This requires excelling in both the information modelling and information management capabilities of BIM, to enable optimum collaboration between stakeholders involved (Sacks *et al.*, 2016a).

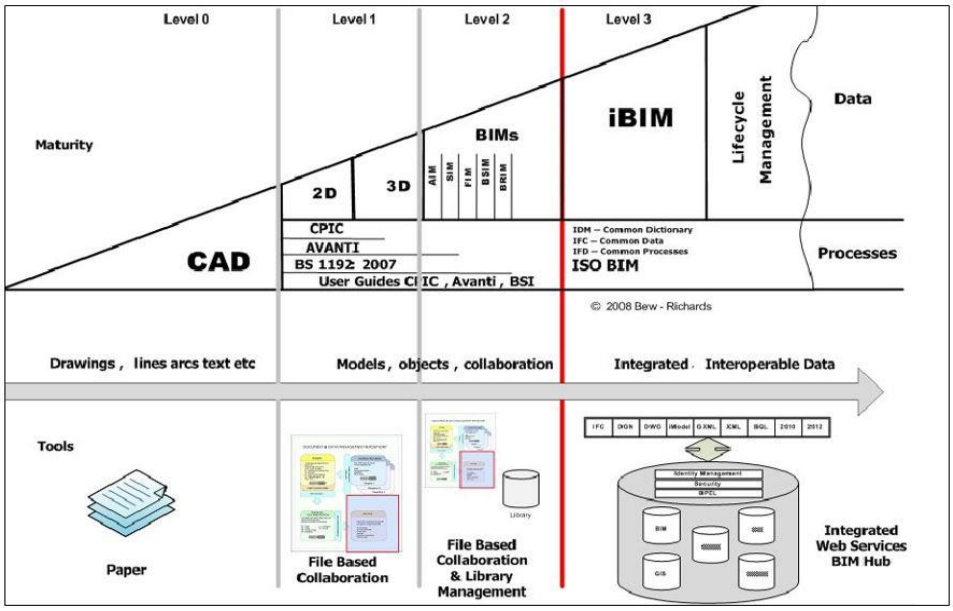


Figure 3- BIM Levels, Source: bimportal.scottishfuturetrust.org.uk

2.2.3 Digital Collaboration in BIM

BIM enables better information management by enhancing collaboration and communications between teams (Ghaffarianhoseini *et al.*, 2017b). With the adoption of BIM, all information is updated on a single data base which can be accessed by all stakeholders involved (Dawood *et al.*, 2009; Hu, 2008; Liu, 2009). This will benefit all phases of a project lifecycle, such as information management in construction sites, which commonly faces issues with managing the exchange of information, (e.g. daily safety reports), generated from various sources, that might contain overlapping information (Chen and Kamara, 2011; Cho, 2002; Lee *et al.*, 2018).

Traditionally, the development of process models was carried out based on ISO standards for the exchange of data between different disciplines (Pratt, 2001). BIM models have a schema (i.e. data structure) that users follow to organise and structure data (Abdelmohsen *et al.*, 2011). In a BIM-enabled project, there are several schema for different products and hence, different information can be exported from various applications for the same object, leading to potential misinterpretations and loss of information within the data exchange processes between stakeholders (Honti and Erdélyi, 2018a). For a successful exchange of information through CDEs, all stakeholders should seek compliance with the regulations and best-practice

guidelines and standards (BSI, 2013a). As best practice guidelines and standards are continuously evolving, The UK BIM framework is developed to assist the industry professionals in transitioning from the previous BS1192 suite to the ISO19650 series which have recently been published. By providing useful resources and guidance documents, UK BIM Framework promotes compliance to the most up to date standards for all industry stakeholders ("UK BIM Framework", 2019).

Collaboration in BIM-enabled projects entail the ability of different systems to exchange and share data in several formats, such as the Drawing Exchange Format and Initial Graphic Exchange Specification (Demian and Walters, 2014). Although there are different data exchange file formats, the Industry Foundation Classes (IFC) is the one that is commonly used in data exchange between different stakeholders (Abdelmohsen *et al.*, 2011; Edmondson *et al.*, 2018; Patacas *et al.*, 2016). A research study carried out by Van Berlo and Hendriks (2012) concluded that IFC contributes to the improvement of workflows especially in integrated project delivery systems, which inherently improves on the consistency and quality of data. Thus, Autodesk and Bentley systems made an agreement to facilitate exchanging files to ease the process of switching between the two products (Interview: Bentley Systems' Greg Bentley, 2016). This enables enhanced coordination and collaboration for the stakeholders involved in working on an integrated model (Theiler and Smarsly, 2018). For example, a project might include engineers from different departments such as: civil engineering, mechanical engineering, planning, and architectural engineering and many more. Each department's input in the model is different and therefore, different end products would be generated, such as master-plan drawings, structural and architectural drawings, building permits, survey drawings, specifications, schedules, cost estimates, and models for visualising the building. All these products and team members interact during the lifecycle of the project creating information of various level of details (LODs) (Karlshøj *et al.*, 2012; Lee *et al.*, 2016). To enable such interactions, a complex digital environment with a large volume of data exchange between different stakeholders is created, where IFC data-exchange files play a crucial role for team collaboration in the AECO sector (Pishdad-Bozorgi *et al.*, 2018). Software companies are continually improving the limitations of IFC data-exchange files in order to make the collaboration easier and more efficient (Bazjanac, 2008; Van Berlo *et al.*, 2012; Theiler and Smarsly, 2018).

All stakeholders (i.e. designers, vendors or contractors) should be transparent as to whether their processes abide with the regulations as set out in the BIM Execution Plan (BEP) (Lin *et*

al., 2016). Similarly, clients should clearly define the requirements for the exchange and flow of data and their strategy for managing information throughout the lifecycle of the project. This strategy should address information management during project execution and operational stages (Radl and Kaiser, 2019; Portal, 2020). Additionally, there might be more than one CDE in a project and each with differing user groups and varying functions. A project might entail a CDE for the exchange of information between a contractor and a designer and another CDE for the client to receive or publish information (BIM portal, 2020b). A CDE strategy related to the operational stage would be called the Asset Information Model (AIM), in which, if applied on an enterprise level would enable clients to access information across different projects while abiding with the regulations of information management as defined by BS 1192-3 (BIM Portal, 2020; Shillcock, 2019). Organisations usually have several projects with indefinite number of team members; therefore, the AIM is a significant investment that would require organisations to understand the requirements of integrating this strategy with the internal processes of the organisation (BIM Portal, 2020b).

Prior to the commencement of a BIM project, clients must investigate their infrastructure capabilities to ensure that data exchange is done efficiently, and the process would be maintained over time (BIM portal, 2020b). As stated in the BS1192-3, the Organisation Information Requirements (OIR) are client information models that include the information required to make strategic decisions (BIM portal 2020c). In OIRs, information requirements are categorised in a way that assists the organisation in managing physical and digital assets (Ashworth *et al.*, 2016). There are several organisational aspects taken into account for the development of the OIR documentation (O'Neil and Saleeb, 2019). The available time and budget required to gather, extract and store data in addition to the tools that are available in order to undertake these processes are all aspects that would be addressed in a business case (O'Neil and Saleeb, 2019). Asset Information Requirements (AIRs) are the building blocks for OIR as stated in BS1192-3. They include detailed information in response to the requirements set out in the OIRs (The BIM Hub, 2018). In order to regulate the flow of data and make it more structured when defining the requirements of OIR, the Asset Information Model (AIM) is created to incorporate the different AIRs in which they are classified and structured to get stored (Amatsari *et al.*, 2017). In order to be able to use AIRs in defining the requirements for OIRs, it is important that they are sufficiently granular from which answers can be derived for different questions regarding the asset's lifecycle (Patacas *et al.*, 2016; The BIM Hub, 2018). Plain Language Questions (PLQs) are defined as per the British Standards Institute as the

questions that are asked by clients through the supply chain of an asset from which decisions can be made. These questions assist organisations in identifying the requirements at various stages of a BIM project life cycle, through the identification of current stance and its comparison to the organisational/project goals (BIM Portal, 2020).

2.2.4 BIM Lifecycle

BIM facilitates informed decision making at early stages rather than late in the process, which inherently reduces wastage of time and resources (Lorimer, 2011). As per the Omni Class Construction Classification System, lifecycle of construction projects is divided into 9 stages which include: idea, concept, design criteria, design, coordination, construction, commissioning, operations and closing (OCCS, 2013). Other resources such as The Royal Institute of British Architects (RIBA) have suggested other phases, in which there are 7 phases including ideation, concept, design, detailed design, construction, commissioning, closing, and using the facility (Sinclair, 2019). Alternatively, some studies recommended a more abstract categorisation using only three phases which are design, construction, and operations (Succar, 2009).

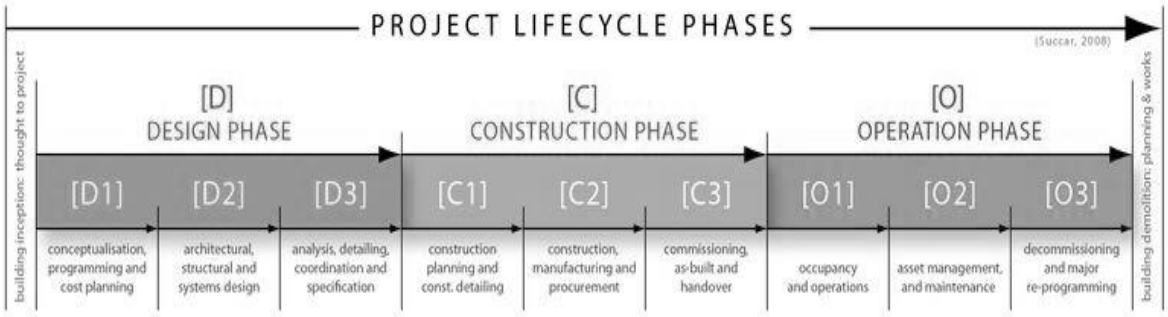


Figure 4- BIM Phases, Resource: Succar, (2009)

As stated by the Construction Industry Council (2013), adopted from PAS 1192, the project lifecycle can be broken down into 7 phases. These include brief, concept, developed design, production, installation, as conducted, and in use (figure 3). These phases can be linked to the delivery of projects. The different stages for project delivery systems were: strategy, brief, concept, definition, design, build and commission, handover and closeout, operation, and end of life (CIC, 2013).

As pointed out in figure 4, BIM models have the ability to combine graphical, non-graphical information and documentation in one file from which a user can define and visualise the components of buildings (Kensek, 2015; Morlhon *et al.*, 2015). BIM models also offer information on how different objects and parameters interact with each other and how they are interrelated (Honti and Erdélyi, 2018b). Hence, this entails data exchange files to contain more information than just simple geometrical information that are usually shown on CAD files (Bandi, 2019).

Research studies have addressed the features of BIM that can be used over the lifecycle of the project. As stated by Baldwin and Bordoli (2014), application of BIM in the design phase enables spatial visualisation and interdisciplinary coordination. BIM can also be used in design analysis for structural elements, energy modelling and simulation, and viability check of the design against the code (Czmoch and Pękala, 2014). During the construction phase, BIM enables informed decision making regarding site mobilisation and utilisation, activity sequencing, scheduling and cost estimation (Eadie *et al.*, 2013). It can also be used in asset and facility management by monitoring, managing and reporting issues that would be linked to the building environment and components (Kelly *et al.*, 2013a).

2.2.5 BIM Data Across Project Phases

In a BIM-enabled project, the project information is visualised in a digital environment to provide useful information for decision making in various activities within a construction project, such as procurement, fabrication, construction and operations, and maintenance (Zhang, *et al.*, 2015). The digital representation of the project is in the form of a model which contains information regarding the geometry, spatial environment, characteristics of building components, cost estimations and many more characteristics of the project (Bazjanac, 2008). The real time update of this model with the progress and advancement of the project allows for the exchange and communication of the scope of the quantities, scope of the work and the potential changes and amendments with all stakeholders (McArthur, 2015).

The information used within every stage of a BIM project is of a different level of detail (LoD). The Level of details (LOD) is defined as the extent of information that can be provided to the user. The term information refers to the geometric and non-geometric information required to complete a certain task in a BIM project (Kim *et al.*, 2013). The LOD has been addressed in several research studies (Calvin Kam *et al.*, 2013; Jeong *et al.*, 2009; Leite *et al.*, 2011). The American Institute of Architects (AIA, 2013) published the E202 LOD standard which can be

used in different lifecycle phases from which the user can determine the LOD level on a five-level scale starting with 100 and ending with 500. This scale indicates the level of details and the richness of the information attached to an object in the model. Information such as geometrical and geographical location can be determined at level 100, whereas level 500 indicates accurate size, orientation and quantity in addition to some detailed information such as time and cost (Ikerd *et al.*, 2013).

Several studies have addressed various classification of LOD. These studies were mostly based on AIA standards. For instance, in the United Kingdom, the BIM Forum adopted the same five levels of AIA standards in developing the LOD specification. An additional level, namely level 350 was added to the five-point scale. Leite et al. (2011), suggested another LOD to be used by software developers in which information such as shape and location geometry and fabrication can be identified. The LOD developed by AIA which has also been presented in different studies, described the different levels and corresponding level of details in each level. In LOD 100, the elements in a model are graphically represented by symbols and generic elements, in a way that does not classify to level 200. In LOD 200, model elements are represented graphically in an approximate way with some information such as quantities, heights, lengths, and widths in addition to geographic orientation. LOD 300 models contain graphical representation for specifics, either a system or object, and information such as quantities, sizes and geographical location are shown. Similarly, LOD 400 contains the same information as the ones in LOD 300, however the user would be able to attach non-graphic information to the elements of the model. LOD 500, would have the model elements size, quantities and location in addition to non-graphic information (Ikerd *et al.*, 2013; Latiffi *et al.*, 2015).

A higher LOD would help in more accurate analysis of performance inside buildings (Autodesk, 2017), which is known as Building Performance Analysis (BPA). If a model is at a LOD 100, this would prevent a user from modelling energy which would be required for LEED certification, however LOD 100 can determine how sunlight would affect energy consumption inside the building. Therefore, LOD and BPA share certain inputs and outputs as the project progresses (Liu *et al.*, 2017). In order to assess a model using BPA, LODs can be determined based on the evolution of the project lifecycle.

In the ideation (planning) phase, project requirements are identified, and aspects related to existing buildings and services are collected (Autodesk, 2020a). There are assumptions related

to LOD at the idea phase during the project lifecycle. For example, if it is an existing project there could be a pre-existing BIM model at level 300, while if it was a new project, the possibility of having a BIM model would be low. In this phase, decisions related to data and geographic location should be made in addition to project site-visitations and investigations. Information related to the climate such as wind speed, daylight duration, precipitation and existing utilities shall be gathered. Following the collection of data, analysis shall be made in order to determine the feasibility of having a building in this location from which sustainability issues can be resolved and analysed (Autodesk, 2020; Grytting *et al.*, 2017; Ikerd *et al.*, 2013; Leite *et al.*, 2011). In the concept design phase, the general idea and direction of how design will progress is set. At this phase, most models are at LOD 100 in which elements are modelled at an abstract level. During this phase conceptual runs are made to predict energy consumption. Studies related to building orientation and facades would also be carried out at that stage (Autodesk, 2020b).

After proposing concept designs, design development is instantiated in which proposed design is refined and materials are selected in addition to the structural elements design (Autodesk, 2020c). In the design and development phase LOD is usually LOD200 or LOD300 in which materials for cladding are identified and wall thicknesses and materials are modelled. At this phase, the structural model should be at LOD200 with structural elements selected and designed (i.e., beams, columns, or frames). MEP models are usually at LOD200 in which pipes and ducts sizing would be the next task (Leite *et al.*, 2011). A complete building analysis and simulation is carried out at this phase in which the geometric features and building components are analysed (Autodesk, 2020c). Also, energy modelling is performed to understand the building reaction to solar radiation based on the selected materials. Additionally, structural analysis is carried out to size structural elements and finalise the design (Autodesk, 2020c). During the final design, detailed design and documentation for the various project components are produced (Grytting *et al.*, 2017). All models should be completed at LOD 300, with sizes and materials finalised on all elements in the building. At this stage, documents for the final design are produced which would include the findings for the final building analysis (Nilsen and Bohne, 2019). During construction phases, the as-built elements would be modelled which would be at LOD 400.

After the construction phase, operations and maintenance for the building requires LOD 500 in which actual operating conditions are accurately represented on the BIM model (Cassano and Trani, 2017). During this phase, commissioning and testing are performed by facility

management in which the comfort for occupants can be determined. The difference between design and actual building performance can be verified and the costs resulting from these differences can be calculated (Alavi and Forcada, 2019). In this phase, facilities- management organisations undertake the operations and maintenance of the facilities, by exchanging high volumes of data with maximum level of detail (Becerik-Gerber *et al.*, 2012a).

2.2.5.1 Security of BIM Data

Explorations of BIM data across various phases of a BIM lifecycle illustrated that high volumes of digital information are managed and maintained in all phases of a BIM lifecycle. The information can be in various formats, with different level of details in the various phases (Dawood et al., 2015). However, the common thread across all phases of a BIM project is the digital collaboration between all stakeholders involved in the project (Ashcraft, 2008). This requires an increased interaction of people (stakeholders) with technology (BIM tools, digital devices and systems), where each stakeholder may be at a different level of BIM adoption, with different information management capabilities and facilities (Succar, 2010). This raises concerns regarding the secure management of BIM data at rest (archived) or in transit (during exchange) (Giel and Issa, 2013). Thus, the following section presents a holistic overview of the issue of cybersecurity in the digital built environment, to explore the cybersecurity risks and threats, and in particular, across various phases of a BIM project.

2.2.6 Cybersecurity across BIM Lifecycle

As stated by Mutis and Paramashivam (2019), many factors contribute to the cybersecurity vulnerability of a BIM-enabled project, which include: BIM level, level of data and how it is exchanged. Therefore, throughout the lifecycle of a BIM-enabled project, risk impact and vulnerability differ, based on the phase that the project is in.

In the early phases of a project planning, the aim is to determine the feasibility and objectives of the project (Mantha and de Soto, 2019; Zhang, Seet, *et al.*, 2015). A feasibility study is carried out after identifying the project requirements, for which the technical requirements are analysed, and preliminary cost estimations are produced. During this phase, the number of stakeholders is at a minimum, with the majority of information being in 2D formats (Akcamete *et al.*, 2019). The LOD in such phases is commonly LOD 100 which entails a relatively lower data-sensitivity in most projects. However, there are still critical assets that deal with data, that could be subject to threats, such as data theft (Kure *et al.*, 2018). Competing parties might be interested in getting their hands on the sensitive financial and commercial information, for

achieving leverage over other parties (Brackney and Anderson, 2004; Sommer and Brown, 2011).

During the design phase, project objectives are implemented in the form of a preliminary design. In this phase, collaboration entails the exchange of information in 2D and 3D formats with a relatively higher LOD (e.g. 200 or 300), because the data is representative of more components, structure and details of the project (Leite *et al.*, 2011). Thus, the level of vulnerability slightly increases in comparison to the start of the project. Also in this phase, critical asset-information, including cost estimations, proprietary data on materials, or design of building components, is subject to theft through unauthorised access, leading to financial losses and reputational damage for the organisation (Baker, 2014; Björck *et al.*, 2015).

A cybersecurity attack in this phase might also result in theft of intellectual properties (Loza de Siles, 2015). Innovative ideas in the design phase of a model, or a certain construction-method statement is considered as intellectual property, and, if an engineer or architect wants to prevent an idea from being exposed or stolen, appropriate security measures should be implemented. As BIM models provide a centralised data base, accessible to all stakeholders, the risk of a compromise of intellectual properties is rather high (Boyes, 2015a; NIBS, 2017).

During the construction and procurement phases, the data is a higher LOD (i.e. LoD 400 or 500) and provides a more accurate representation of the project components and environment (Aram *et al.*, 2013; Lin and Su, 2013). Therefore, a breach of cybersecurity could allow malicious tampering with data regarding the equipment and machinery, resulting in disruption of operations, or health and safety implications for the workers on site (Boyes, 2015c). Remote access to data using mobile devices connected to the internet, is also associated with risk of cybersecurity compromise. The connection to the public-internet networks would increase the vulnerability of devices to attacks using malware (Vishwakarma, 2016). Hence, the use of mobile devices to access a BIM model on site are accompanied by cybersecurity risks (Lin and Su, 2013).

Following the delivery of the project and during its in-use phase, facilities are maintained and operated in order to avoid degradation over time and to maintain a certain level of functionality (Apostolopoulos *et al.*, 2016; Marmo *et al.*, 2019). During this phase, the data for the facility, including all devices and components installed, are stored and exchanged with a large number of stakeholders (Mayo and Snider, 2016; Tang *et al.*, 2020). This data is of the highest LOD, as it represents both the as-built, and as-maintained information for the facility (Alavi and

Forcada, 2019).The connectivity of BIM with building management systems that control the IoT devices installed within a facility, may enable malicious cyber actors to perform cyber-attacks, with the aim of causing physical damage to the facility or a threat to the health and safety of the occupant (Cui *et al.*, 2018; Yaqoob *et al.*, 2017). The damage can take the form of financial loss, reputational loss, operational disruption, security breach, injury or loss of life of the occupants (Amin, 2019). Hence, the impact of a cyber-attack during the in-use phase of a BIM project is deemed as critical.

The BIM life-cycle cyber-risk model (Figure 5) portrays various phases of a BIM lifecycle and their attributed LOD, information content and potential cyber-risk impacts at each phase. It also demonstrates a holistic view of the issue of cybersecurity, by presenting the risk impacts at each stage and highlights the life span of each phase to enable comparison.

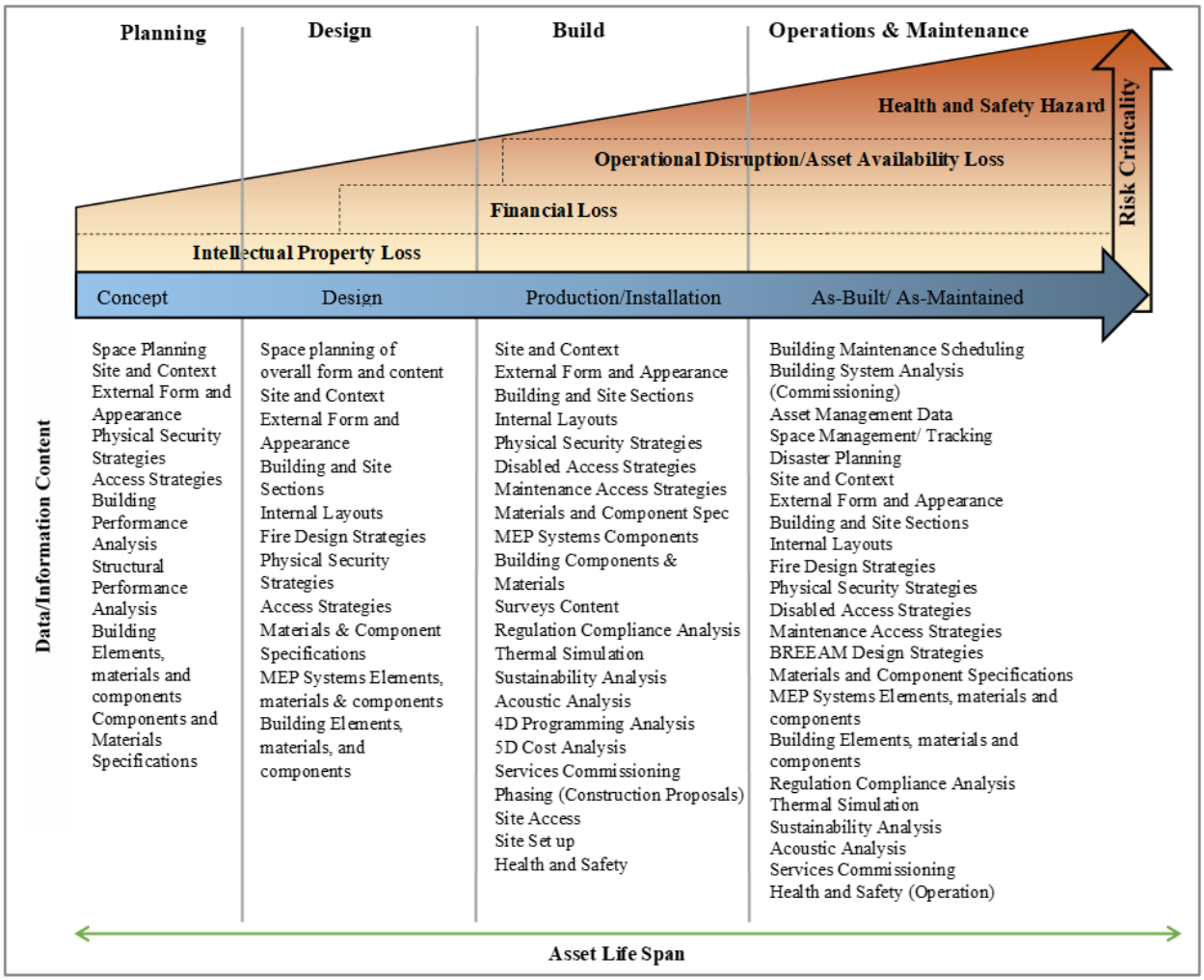


Figure 5- Conceptual Cybersecurity Risk in a BIM Project (Whole Lifecycle)

Figure 5 illustrates that cybersecurity risks impact all phases of a BIM lifecycle. Although the impact of a cybersecurity risk in earlier phases is not as critical as the final phases, they may still have disastrous effects on the facility and those involved in the project. However, as the in-use phase is found to be the most critical, in terms of the impact of cyber-attacks, the focus of this research is narrowed down to the BIM-FM organisations. This enables the research to conduct a more focused investigation into the problem and collect concise knowledge on the cybersecurity management of BIM-FM.

A summary of the findings that support the decision made above are listed below (Alavi and Forcada, 2019; Amin, 2019; Apostolopoulos *et al.*, 2016; Cui *et al.*, 2018; Marmo *et al.*, 2019; Mayo and Snider, 2016; Tang *et al.*, 2020; Yaqoob *et al.*, 2017) :

- A very high volume of data is exchanged and stored in the facilities management organisations
- A long-term (more than 10 years) of data life cycle is estimated for the in-use phase.
- The facilities management working processes entail collaboration with various contractors, suppliers and providers of products and services. Hence, data is digitally exposed to various stakeholders involved in a BIM project.
- An increase in the physical security risk due to smart devices and sensors installed in the buildings, which can cause danger to the health and safety of personnel and residents of the facility.

Considering the findings, the secure management of information at the in-use phase of a BIM project would be critical. Therefore, robust information management processes and procedures are required to ensure the availability of information to achieve the BIM benefits in FM. To further understand the issue of cybersecurity in BIM-FM organisations, the following section presents an overview of the application of BIM in FM, to implementing BIM in FM, and to understand the challenges associated with the implementation of BIM in FM organisations.

2.3 Role of BIM in Facilities Management

2.3.1 Overview of Facilities Management

Facilities management organisations are involved in multidisciplinary tasks to deliver functional working-environments that accommodate people, processes and technology (British Institue of Facilities Management, 2012). Existing studies propose varying definitions of facilities management. While some studies consider more tasks areas, others only focus on a

limited number of activities associated with FM. In the light of this, Shiem Shin Then (1999) describes facilities management as a practice that seeks to provide a functional environment for the support of businesses and their resources. The author further elaborates on the role of facilities managers, which is to balance all assets inside a facility by delivering the needs and overcoming the challenges. Many resources such as the Omni Class Construction Classification System (OCCS) distinguish between the management of facilities, and their operations and maintenance tasks (Services, 2018). In the light of this, facilities management is defined as the management of safety and functionality of facilities, which differs from the operations and maintenance tasks that are solely focused on maintaining the operations within the facility (Succar *et al.*, 2013). Alternatively, several resources present a more comprehensive definition of FM, which includes maintenance and operations as part of the FM's activities to ensure the functionality and usability of buildings (Barrett and Baldry, 2003; Becker and Steele, 1990). Some authors have even proposed that facilities management can also include all the stages of a construction project (Ebinger and Madritsch, 2012).

2.3.2 BIM-Enabled Facilities Management (BIM-FM)

In traditional facilities management, information, including equipment inventory, data sheets, spare parts and schedules used in maintenance activities, are usually paper based documents that are handled and exchanged manually (Abdullah *et al.*, 2015; Wang *et al.*, 2013). Such information is sometimes incomplete and inaccurate as a result of human error. Hence, huge efforts are required to recreate these paper-based documents if they are lost or damaged (House *et al.*, 2007; Keady, 2013). Carbonari *et al.*, (2018) highlights that BIM resolves this issue by providing access to all the required information through a digital platform which enhances communication and collaboration amongst all stakeholders (Lin *et al.*, 2016; Matarneh *et al.*, 2019). However, this depends on FMs understanding of the information requirements of each task (Volk *et al.*, 2014). Patacas et al., (2015) point out that the early engagement of FM in a BIM-enabled project facilitates the coordination of all phases of the construction project by coordinating workflows, tools, and regulations to fulfil the information requirements of the FM tasks (Eastman et al., 2011). This will ensure the right data is shared with the right stakeholders, to save time and effort in finding the right data for a specific task (Lin *et al.*, 2016).

The visualisation capabilities brought by BIM enables an improved understanding of the building components compared to the conventional 2D drawings (Leite *et al.*, 2011). A BIM model visualises the updated as-built and as-maintained information of a facility, including the

Mechanical, Electrical and Plumbing (MEP) data required to perform operations and maintenance tasks (Hu *et al.*, 2018). Also, BIM models provide parametric description of the interrelationship between the components, enabling the management of the building performance and monitoring the functionality of the components (Abdullah *et al.*, 2015; Atkin, B., & Brooks, 2015; Gao and Pishdad-Bozorgi, 2019). These features in BIM provide enhanced accuracy on the predictions and estimations of the resources required for undertaking all FM tasks (Marmo *et al.*, 2019)

The review of the literature demonstrated that the implementation of BIM, benefits the FM organisations in various task areas (Pishdad-Bozorgi *et al.*, 2018). As per the definitions in section 2.3.2, activities in task areas differ across FM organisations. They might focus solely on management and maintenance of the operations and functionalities of the facility, or might also carry out renovations and construction projects (Barrett and Baldry, 2003; Ebinger and Madritsch, 2012). However, despite the high variety of activities carried out within various FM organisations, the literature is commonly focused on the benefits of BIM in financial management, space management, and the operations and maintenance of facilities. According to Barrett and Baldry, (2003) and Becker and Steele, (1990), the FM task areas include the operations and maintenance, as well as the management of the physical and digital assets. However, as per Ilter and Ergen (2015), the sustainability projects in the built facilities and those projects involving refurbishment and renovation, can neither be fitted in operations or management. Hence, space management is considered as an individual category which includes management of space and optimising the utilisation of environments within a facility. Therefore, the following sections will provide an overview of the implementation of BIM in three main task areas of FM:

2.3.2.1 Financial Asset Management

Facilities management is not only limited to managing and maintaining the physical assets of a built environment, such as the heating system, it covers the management of all assets related to a built facility, including cost estimations, structural data and data related to occupants and operations (Guillen *et al.*, 2016). In this regards Eastman et al. (2011) and BIFM (2012), suggested that the implementation of BIM in FM could be used to support real-time decision making, regarding resource allocation, scheduling, and financial management.

The asset-management task area in a BIM project involves managing the finances as well as the contractual documentation and legal matters for the facility (Kassem *et al.*, 2015a). Costs

for preventive and corrective maintenance must be identified right at the outset. The BIM model sets up cost control for facility managers and establishes an effective monitoring system for the management and control of the budget (Naghshbandi, 2016a).

For the optimum management of assets, data should be collected and maintained for all systems and services, that need to be continuously running to keep the building functional. Asset management entails documenting and storing as-built drawings, lists of equipment and their spare parts, warranty certificates, defect liability periods of contractors and suppliers, contact details of suppliers, operation and maintenance manuals, product data-sheets, a preventive maintenance schedule and other asset-specific information that assists with the effective management of the physical (tangible) and digital (intangible) assets related to a facility (Becerik-Gerber *et al.*, 2012b). The availability of accurate information in BIM-FM would enhance the asset value by enabling effective FM (Guillen *et al.*, 2020). This is achieved through the effective management of budget and human resources and the timely maintenance of the facility, which improves the life-span of the built asset (Alkasisbeh and Abudayyeh, 2018).This requires concise information about material quantities, and the labour costs required for undertaking a specific task, which can be facilitated by BIM (Tang *et al.*, 2020).

2.3.2.2 Space management

Space management involves the optimisation of the way space is used in a facility. In the light of this, Steiner, (2006) states that the management of space and the physical assets within, can have a positive or negative impact on the productivity of workers within a business environment, or the comfort of residents in any type of facility.

One of the most desirable features of BIM is its capability for visualising space and its components, enabling optimised planning of the requirements of space utilisation (Becerik-Gerber *et al.*, 2012b). In this regards, ARCHIBUS (2013) elaborates on the need to have an accurate inventory of all assets associated with certain spaces of a facility, including the asset description along with the status of the space being used, or left unused. This information is often in the form of a CAD file, along with specific indexes that are used to collect, or display data related to a specific space within a facility. BIM assists by accommodating elevation creation, section modelling, layout views and visual rendering of the proposed changes; and hence, results in time saving and cost-efficient decision making (Love *et al.*, 2014). One of the identified challenges in this regard is inconsistent labelling and updating of information, which can be resolved by the effective application of BIM in FM (Becerik-Gerber *et al.*, 2012b). An

additional benefit of BIM in FM is the potential to monitor asset utilisation over the period of use. This would show that the space is both sufficient and meets the user requirement (Ashworth, Tucker and Druhmann, 2016). Furthermore, BIM provides access to information about the building structure and shell, entailing the load calculation for structural elements (column, beam, slabs, core wall and shear wall) and assisting facility managers in decisions on major renovations (McGraw Hill Construction, 2012). It is also possible to verify the material selections against the specific building code and regulations (AEC (UK) Committee, 2012).

2.3.2.3 Operations and maintenance

According to Barbarosoglu and Arditi, (2019), operations and maintenance of a facility is either corrective or preventive. Preventive maintenance encompasses services that prevent failure of machinery or components in the future; while corrective maintenance corresponds to actions that are taken to maintain the operations of a facility (Kassem *et al.*, 2015b; Sullivan *et al.*, 2010; Yam *et al.*, 2001).

BIM enables the real-time exchange of facility information for all the stakeholders involved (Matarneh *et al.*, 2019). The real-time information is captured from various digital tools used in FM to optimise working-processes (Pishdad-Bozorgi *et al.*, 2018). For instance, CMMS and CAFM, as two of the most commonly used software in FM, are capable of storing built-asset information for reactive and preventive maintenance as well as tracking and monitoring events (Mohanta and Das, 2016). This information will be updated on the BIM model to enable improved decision making, leading to the optimisation of processes and work plans within the operations and maintenance tasks (Carreira *et al.*, 2018).

Furthermore, operational management requires continuous and real time monitoring of the facilities, which is where BIM plays a critical role (Davtalab, 2017). The real-time sensing of the smart devices integrated with BIM 6D-models can save time by up to 80% (Davtalab, 2017), enabling the optimisation of processes in operations and maintenance tasks. The accurate assessment of the asset, including the resource limitations, and the accurate evaluation of the conditions of the asset, assists the facility management-team to model and predict the deterioration and depreciation of the assets. Furthermore, the repair and maintenance strategies can be selected by also taking into account the requirements and risks involved in the processes (Naghshbandi, 2016a). In this regards, Lavy and Jawadekar (2014) point out the capability of a BIM 3D database in providing useful information that could assist in the prediction of building behaviour and facility deterioration more accurately.

BIM simulation capabilities enable the creation of multiple replications for different energy-use scenarios, and the reaction of facility-systems to each scenario to enable the enhancement of the system configuration. For instance, using such an approach would facilitate corrective measures when a certain space is unoccupied, such as switching off the lights, which would eventually reduce energy consumption and result in energy savings. This could also be used to predict energy consumption over time, based on previous trends of consumption and usage (Gourlis and Kovacic, 2017; Wu and Issa, 2015). In addition, the building-performance data collected through BIM ensures that the building is operating as per a specific standard. The areas to be modified or upgraded could be identified by the FM team to improve the overall building-performance (Carnero and Gómez, 2017).

In maintenance management, BIM assists FM to implement a proactive-maintenance plan. The facility managers can develop efficient maintenance plans as well as keeping a record of maintenance, which will ultimately reduce any corrective and emergency maintenance (Carnero and Gómez, 2017). In complex building structures where several systems are working simultaneously, essential services cannot be halted for maintenance, due to the risks involved with health and safety and security. Analysis of BIM models enables FM to undertake a risk assessment for operation and maintenance processes, leading to improved coordination amongst the contractors, suppliers and inter-organisational teams (Becerik-Gerber *et al.*, 2012b).

Emergency management is another important task area which benefits from the implementation of BIM in FM (Arslan *et al.*, 2014; Gao and Pishdad-Bozorgi, 2019; Wang *et al.*, 2014) Emergency events, both human or natural, such as: failure of services, fires, earthquakes, and force majeure need to be managed, in order to avoid business disruptions, health and safety compromise or financial losses (Federal Emergency Management Agency, 2003; Lee *et al.*, 2013). Emergency management relies on up to date data from different sources which would need to be well organised and maintained to enable an informed and appropriate decision in the event of an emergency (Federal Emergency Management Agency, 2003; Kennett *et al.*, 2005).

Being able to access the data from BIM quickly can give insights which enable prompt decisions. Through the visual capabilities of BIM models, users can identify the location of events and pinpoint the hazards or identify the interrelationships between hazardous locations and emergency-evacuation routes, to aid decision-making during emergency events (Wang *et*

al., 2014) . Additionally, BIM can contribute to the development of better training for emergency management (Becerik-Gerber et al., 2012). The simulation capabilities of BIM can be used to simulate the expected impact of an event and testing the anticipated responses for the proposed emergency plans (Arslan *et al.*, 2014; Chen *et al.*, 2020).

Table 1 summarises the benefits associated with the implementation of BIM, in the three main task areas of Financial Asset Management, Space Management, and Operations and Maintenance:

Table 1-BIM benefits in FM

	Task Area	**Potential BIM benefits**
BIM-FM	Financial Asset Management	1. Enhancing productivity 2. Improving forecasting and cost estimations 3. Informed decision making 4. Process optimisation 5. Availability of real-time data for cost estimation 6. Visualisation for project elements that must be estimated
	Space Management	1. Increasing efficiency of allocated spaces in a facility 2. Process optimization for building uses 3. Efficient planning of spaces, components, and events 4. Monitoring space use to make improvements 5. Effective management of safety and security of facilities
	Operational Management	1. Developing and visualizing various scenarios to improve building performance and functionality 2. Effective disaster management enabled by the availability of reliable real-time information 3. Availability of updated information regarding facilities' components and equipment 4. Ease of access to the required information for operations and maintenance 5. Availability of accurate quantity take offs 6. Real-time update of the model to include changes 7. Optimisation of maintenance scheduling, monitoring and management to save time, cost and labor

2.3.3 BIM Challenges in FM

Despite the benefits associated with the implementation of BIM in FM, as with any new digital solution, there are strategic, implementational and performance related complexities and challenges which need to be discussed. These include:

- Lack of data availability: It was reported by Becerik-Gerber et al. (2012) and Kassem *et al.*, (2015) that the full potential of BIM in FM bloom with the involvement of FM organisations in the earlier phases of the project. However, current practice demonstrates a lack of engagement by the facilities in the planning, design, and construction phases, in which the information required for the FM operations and maintenance are defined (Gao and Pishdad-Bozorgi, 2019). Furthermore, FM depends on using meaningful data from BIM data models, but sometimes this data is not structured for use within FM working-tasks (Carreira *et al.*, 2018).In many UK public projects, common practice entails changing the FM contractor every 3-5 years (FBIFM, 2010), which could increase the likelihood of poor data transfer from one organisation to the other, resulting in the loss of data or compatibility issues. Hence, additional surveys would be required incurring additional costs (Kelly *et al.*, 2013a). In some instances, contractors are required to conduct a survey of the facility after the completion of construction works, or when a new contract for performing maintenance activities is awarded and the contractor is changed, both of which might result in data duplication (Barbosa *et al.*, 2016). As such, with information not being available at the right time, a BIM-FM organisation will face restrictions in carrying out everyday tasks (Kassem *et al.*, 2015a).
- Lack of organisational BIM-readiness: The cultural aspect of adopting a new technology is also considered a challenge, as FM is considered by many practitioners as a rigid industry with a fragmented nature (Daniotti *et al.*, 2020; Newswire, 2020). This has led to a degree of scepticism and reluctance towards the adoption of BIM, which weakens the cultural readiness of the FM organisation for a digital renovation of working practices (Abbasnejad *et al.*, 2020; Edirisinghe *et al.*, 2017). As stated by Kelly *et al.*, (2013), there is insufficient demand for using BIM in FM, as a result of the costs incurred for facilitating the resources for BIM implementation.
- Lack of knowledge and Skills: To achieve the full potential of BIM implementation, FM organisations are required to provide continuous training programs to upskill employees and ensure they have sufficient knowledge, skills and

awareness in handling, manipulating, interpreting, analysing and managing BIM data and models in FM (Becerik-Gerber *et al.*, 2012b; BIM Task Group, 2012). Considering that BIM in FM has only recently been introduced, there is a gap of knowledge and awareness amongst those in FM industry, which affects compliance to good practice and creates process inconsistencies amongst the stakeholders (Puolitaival and Forsythe, 2016).

- Lack of standardisation: A number of guidelines are available that address the application of BIM in FM organisations (Ashworth *et al.*, 2016; BuildingSMART, 2010). Examples include the Government's Soft landings (GSL) FM guidance, that demonstrates how BIM could be used to support FM throughout the lifecycle of the facility (BIM Task Group, 2012). Also there is the RICS strategic plan of work for BIM in FM, which provides facility managers with the steps to follow for the operations and maintenance of the buildings (RICS, 2017, 2018). However, a number of studies have shown that the existing BIM standards are still developing and need upgrading to address all aspects that need to be taken into account (Alreshidi *et al.*, 2017; Binesmael *et al.*, 2018). To exemplify further, the only guideline addressing the cybersecurity of BIM-FM organisations are the PAS1192-5, later superseded by ISO19650 (New BIM Standards - ISO19650, 2020), which does not specifically address FM practices, and are rather focused on the design and construction phases, and the hand-over of the project data in between the phases (Shillcock, 2019). Furthermore, Sacks *et al.*, (2016) point out that the available standards are evolving and advancing as more FM organisations with various characteristics are seeking to adopt BIM for various FM task areas. This has resulted in difficulties for the FM organisations to standardise their processes and procedures. Particularly in the area of information management in BIM, ISO19650 has been developed in two parts to supersede all previous standards (New BIM Standards - ISO19650, 2020). However, the regulating bodies are still in the process of developing guidelines to assist organisations in complying with the new standards (UK BIM Framework, 2020). As stated by the Centre for Digital Built Britain, (2018), transition to the new ISO standards will require trained resources, as well as financial resources to support the new changes.
- Issue of interoperability and incompatibility: The issue of interoperability and incompatibility of digital project data exchanged between project stakeholders, is one of the challenges of using BIM in FM (Pärn *et al.*, 2017). The British Institute of

Facilities Management, (2012) reported that there is a need to standardise libraries that can be used in data exchange and transfer of data for facilities. The inconsistency and incompatibility of data format and system configuration is one of the challenges that FM organisations face in converting to a BIM-enabled FM organisation (Hoang *et al.*, 2020). For instance, the COBie specifications for exchanging information was developed to capture and exchange information required by FM teams (Kensek, 2015). It was concluded by Patacas *et al.,* (2016) that COBie is used in data structuring to help in overcoming the issue of interoperability, however the lack of knowledge or process for collecting the right data impedes the potential advantages of complying with the standard (Lavy and Jawadekar, 2014).

- Lack of formal documentations and contracts: There are several legal risks that could arise from using BIM in FM such as BIM data ownership and how to protect the data copyrights (Eadie *et al.*, 2015). This is identified as a gap in contractual documentation, that creates complexities in managing access to information for all stakeholders involved (BIFM, 2012). Considering the collaborative nature of the BIM projects, over-restricting access to information may limit real-time collaboration, and create difficulties in managing the security of the embedded data that requires various parties to access the models for validation purposes (AIA, 2013).

2.3.3.1 Invoking the Risks of Cybersecurity in BIM-FM

Challenges in the implementation of BIM are also the contributing factors for a weak information security. For instance, a lack of defined information requirements for FM tasks would lead to the exchange of a large volume of facility-related data amongst the stakeholders, without considering the relevance of that information to the task. Hence, effective authorisation of access to data would be difficult to achieve (Gao and Pishdad-Bozorgi, 2019; Mell and Grance, 2011). The literature further sheds light on the issues associated with transfer of data when the FM body is transferred to a new contractor. The interoperability issues as well as the probability of information loss resulting from the poor handling and management of digital information, heightens the risk of unauthorised access to the data and the compromise of information confidentiality (Mantha, 2020). Also, reluctance to adopt the digital ways of working brought by BIM, further affects the organisational approach for developing the required knowledge, skills and awareness for working with digital tools in a BIM-FM organisation (Akbarieh *et al.*, 2020). This shows that poor interaction between people and technology creates opportunities for malicious cyber-intrusions which compromise the security

of digital data in BIM projects (Doneda and Almeida, 2015). To further exemplify the effect of these challenges on the information security of FM organisations, the literature highlights the issue of interoperability and incompatibility. This results from process inconsistencies and poor compliance to standards and best-practice guidelines such as COBIE, which instruct on how to follow a more homogenous approach to the structuring and layering of data, to avoid complications during the exchange of data and models (Lee *et al.*, 2018; Patacas *et al.*, 2015). A lack of formal documentation stating the process requirements and contractual agreements solidifying the stakeholder responsibilities and authority over the project, also results in complexities with data-ownership. This can further complicate the effective management of data-access authorisation. Data-ownership complexities mean that the responsibility for ensuring the security of the data is lost and hence, the vulnerability of data to security breach increases (AIA, 2013). As stated by von Solms and von Solms (2018) information security should encompass cybersecurity, when the information is presented in a digital environment, but the existing literature has often viewed cybersecurity through an information-security lens (Calder, Alan ; Watkins, 2019; Saleh and Alfantookh, 2011). In a BIM-FM organisation where information is digitally produced, handled, and managed in a CDE, using various digital tools and technologies, a lack of robust information-security management can lead to a heightened risk of cybersecurity breach. The cybersecurity risks and their impact on BIM-FM organisations are further explored in section 2.4.3.

2.4 Cybersecurity Concept in Digital Built Environment

The existing literature fails to provide a unified definition for cybersecurity (Bayuk, 2012), which presents a variety of viewpoints, ranging from technical measures to managerial functions which protect information from unauthorised access (Bailey *et al.*, 2015; Bayuk, 2012). The Task Force Transformation Initiative (2015) presents a more comprehensive definition of cybersecurity as a "computing-based discipline involving technology, people information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p.1).Accordingly, some researchers have also pointed to the continuous prevention, detection and recovery required to maintain the confidentiality, integrity and availability of information, which may be compromised as a result of a breach of cybersecurity (Gerber *et al.*, 2001; Humphreys, 2008; Posthumus and Von Solms, 2004)

A breach of cybersecurity resulted from a cyber-attack is known to adversely affect the functionality of digital systems and devices (Nye, 2018). Gandhi *et al.*, (2011) defined cyber-attacks as any outside attacks that could compromise the security of an organisation or a system inside an organisation. Malicious cyber-attacks are acts carried out with the intent of destroying the user data and documentation (Mayo and Snider, 2016; Wood, 2000). A cyber-attack, if successful, allows unwanted access to data or systems by unauthorised actors, resulting in potential loss of information integrity and availability (Boyes, 2015a; Mantha *et al.*, 2020).

In managing cybersecurity, both cybersecurity threats and risks should be identified. A cybersecurity risk is conceptually defined as the likelihood of an adversarial event and its consequence, resulting from a successful cyber-security attack. For instance, loss of information integrity and its effect on a system or organisation. A cybersecurity-threat is an agent which exploits the vulnerabilities and weaknesses and results in accidental or intentional damage to a system or organisation. Accidental or unintentional threats such as human error in handling digital information can lead to a risk of information leakage or risk of financial damage to an organisation. The following sections will provide further insight into the cybersecurity threats, the risk they pose to systems and organisations and the consequences associated with the risks.

2.4.1 Cybersecurity Threats

Cybersecurity threats are commonly categorised by the techniques used by their initiating agents (Griffin, 2019). Threat agents include people or entities who exploit one or more vulnerabilities in a system or organisations, using various techniques (Bowen *et al.*, 2011). Threat agents which intentionally initiate an exploitation may have various financial, commercial, political, personal, or national motivations. Unintentional threat agents are people who accidentally exploit a vulnerability as a result of a human error or carelessness (Borky and Bradley, 2018). Unintentional threat agents are often an insider threat and a vulnerability/weakness (incompetent and/or careless employees) used by intentional threat agents to compromise the cybersecurity of a system (Brackney and Anderson, 2004).

Intentional- threat agents are malicious insiders (disgruntled employees), hackers, organised crimes, terrorists, and advanced persistent threat (APT). Malicious insiders are commonly disgruntled employees who seek revenge or other financial gains from incurring damage to the information or systems, or to steal data (Scully, 2011). These are often undetected as they have been granted access to system. Hackers and organised crime organisations seek to compromise

security of digital data with the purpose of financial gain and/or blackmailing purposes (Brackney and Anderson, 2004). The advanced persistent threat agent (APT) attackers execute their attack over a long period time, to thoroughly intrude and gain full access and control over the systems and data of the victims. APT attackers have a wide range of intentions including commercial, political, military, and financial. Finally, terrorists are the attackers whose intentions are to inflict harm on the targeted system/organisation/asset, as part of a political campaign, or specific belief, etc. (Hussain *et al.*, 2020).

Threat agents use a variety of techniques to attack organisations through the exploitation of vulnerabilities related to technology, processes or people. (Kopp *et al.*, 2017). These include:

- Social engineering: This is executed by deceiving employees to expose sensitive information or avoid a cybersecurity measure (Griffin, 2019). Insider threats (people) inadvertently allow an attack to take place as a result of their naivety, lack of knowledge, or carelessness (Stanton *et al.*, 2004). As an example of social engineering, phishing attacks have previously compromised passwords and user identification details to compromise security of data and systems (Srinivas *et al.*, 2019). There is an alarming increase in identity theft and systems breaches as a result of exposing passwords. Breaches as such commonly occur, using various phishing tricks by the attacker to collect the victim password by creating fake password fields (Nokhbeh Zaeem *et al.*, 2017).
- Ransomware: Similar to crimes that involve kidnapping and demanding ransoms, ransomware attacks are cyberattacks in which data is held for ransom (Song *et al.*, 2016). In these attacks, the digital information of the victim is encrypted by the attackers and a ransom is demanded and when the ransom is paid, the information is decrypted so it can be used again (Brewer, 2016). This type of cyber threat can be aimed at any digital platform or system, including local drives or cloud-based data storage systems (Al-rimy *et al.*, 2018). Another implication of such an intrusion is that attackers could move between files and computer systems on a network without requesting access, which would result in higher numbers of encrypted data and files (Richardson, R., and North, 2017). In extreme cases, victims are denied access and unless the user has a backup for the affected BIM data and models, there is no other choice except to pay the attacker the ransom which does not guarantee the retrieval of the data in a format that would be fit for use (Al-rimy *et al.*, 2018; Sophos, 2014; Yaqoob *et al.*, 2017).

- Viruses and malware: Acomputer virus is a computer code that is stored on a computer that becomes the host for the virus (Stallings and Bauer, 2011). Viruses are designed to damage the host computer, or collect and send information from the host computer to other computers (Srinivas *et al.*, 2019). Malware is a type of virus that affects the performance of computers and can be transmitted from one computer to another by downloads of software or files from the internet, email attachments in which malwares are embedded, media files that could be transferred from removable devices, or propagation from within the malware itself (Cisco, 2018). Outdated software and hardware which is unable to detect or protect against newly advanced threats, as well as untrained users who bypass security regulations, are enablers of a successful virus and malware attack.
- Denial of Service (DoS) attacks: With the increase of organisations who adopt cloud systems as the base of their operations, attackers target vulnerable systems with 'bugs' by sending inputs to crash or disrupt the system. In such attacks, organisations will not be able to use or access information or systems until they are recovered from backup storage.

Considering the increased sophistication of cyber-threats today and the rapid empowerment of the malicious cyber-intruders, current data management techniques and security measures are insufficient to protect systems against malicious cyber-attacks (Mantha *et al.*, 2020) Technological cybersecurity measures such as firewalls and other software and hardware technical measures often struggle to protect the systems and networks from inter-organisational threats (Rivera, 2017). The insecurities within the infrastructure of organisations has led to billions of dollars of investments on technological cybersecurity solutions, whilst the insider threat is yet the most common reason for cyber incidents (Huber *et al.*, 2009; Lesk, 2011). Recent studies indicate that most cyber incidents, including cyber-attacks and fraudulent behaviours have human error at their core as the initiative of the incident (Huang and Pearlson, 2019). Neglecting the effects of the interactions of people with digital technology, on the cyber security of digital space, has left the doors open to threats and potential risks to organisations and their assets (Rowe and Garfinkel, 2012).

2.4.2 Cybersecurity Risks

Cybersecurity risks and the potential threat they represent are often associated with loss, damage, interruption, or destruction of a data/asset/ system. A cybersecurity threat poses risk

to the confidentiality, integrity and/or availability of information, which is accompanied by adverse implications for the affected organisation (Cabric, 2015). This is known as the cybersecurity triad or CIA, which is a classic model that is widely used as the foundation of managing digital information (Henderson, 2019). The three aspects of confidentiality, integrity and availability (CIA) of data are essential to the value of the information and digital assets (Sherman *et al.*, 2017) and contribute towards the operation of the assets within or related to an organisation (Salminen, 2019). Thus, compromising any one of the components of the triad may incur adverse implications, such as the degradation, malfunction, abuse and unavailability of the targeted asset (Couce-Vieira *et al.*, 2020).

- Risks to data confidentiality: Confidentiality refers to the authority of people who are allowed to access and view the data. Confidentiality of data may be compromised by an unauthorised access to the information, whilst sitting in the archive, or whilst being transferred and/or used by the users. This can be facilitated by various attack methods, such as a successful phishing attack that exploits user credentials to gain access to information/ systems. It can also result from an infected tool such as a USB, physically inserted in a device to capture input data (e.g., keyboard sniffer). An infringement of information confidentiality regarding the intellectual property or sensitive commercial-data can result in financial and reputational losses for the organisation (Winzar *et al.*, 2018). A leak of sensitive organisational information can also result in financial blackmail for the organisation (Couce-Vieira *et al.*, 2020). Furthermore, organisational information also includes personally identifiable data which, if obtained by criminals, could result in harm to clients, employees, and communities and in some instances, could result in fines and/or regulatory complications for the business.
- Risks to data integrity: Integrity is concerned with unauthorised changes to data, infringing its validity while it is transmitted, processed, or archived. This infringement may be carried out by unauthorised modification, addition, corruption, and manipulation of data, which results in the malfunction or disruption of operations in an asset or system. As stated by De Sá *et al.*, (2017), malfunction or degradation of an asset results in a reduction in productivity, or disruption to its functions, with the aim of incurring financial losses and/or negative commercial implications for the targeted organisation. Infringing the integrity of data also refers to the manipulation of an asset (e.g., systems, devices) to produce undesired outcomes. An example of this is an unauthorised access to a greenhouse smart temperature-control to dramatically increase

or decrease the temperature, with the aim of causing harm to the plants and resulting financial loss (Axelrod, 2013; Kure *et al.*, 2018). The adverse implications of a breach in an environment such as a smart building, occupied with people could also have health and safety implications (Minoli *et al.*, 2017).

- Risks to data availability: The availability of data is to ensure the required data is accessible to authorised people, in the right format and at the right time (Kumar *et al.*, 2016; Olivier, 2002). A compromise of availability refers to the disruption or obstruction of systems or processes, which could pose a range of unwanted effects on the organisations and their clients (Couce-Vieira *et al.*, 2020). Depending on the targeted asset and its purpose, the implications can vary from financial losses, to injury and death. If the targeted asset is a production machine, the implications are limited to financial and reputational loss for the organisation. However, when a disaster, such as a fire, occurs in a facility, not having up to date information available, could have health and safety implications for the occupants (Ahmad Zawawi *et al.*, 2014).

Cybersecurity risk management plans are often based on CIA, which is used as a reference point (Aminzade, 2018), however, managing a balanced approach towards the three aspects is proven to be challenging for many organisations (Aminzade, 2018). Excessive measures to protect the confidentiality and availability of data would negatively affect the availability of data required for undertaking authorised tasks (Tagarev, 2020). Therefore, in managing the balance between the three aspects, awareness of the potential implications of the cybersecurity threats is essential (Aminzade, 2018). This will enable the organisations to determine their preparedness to accept risks to a certain extent, when considering the business goals and objectives (Kosseff, 2018; Olivier, 2002)

2.4.3 Risk Matrix: Cybersecurity Risks for BIM-enabled FM

The review of the benefits associated with the implementation of BIM in various task areas of FM, highlighted the importance of data availability and accuracy (Section 2.3.2). The as-built info-graphic BIM model of the facility includes data for the devices, installations, and fittings as well as detailed 3D models of various elements incorporated into the building (Matarneh *et al.*, 2019). The availability of real-time data for the facility as it is maintained, and the integrity of that information is key to achieving the potential benefits of BIM (Kelly *et al.*, 2013b). Therefore, a breach of cybersecurity, infringing the integrity and availability of data would compromise the potential benefits of BIM in FM. For instance, the availability and accessibility

of accurate and up to date information for the facility in a BIM model, optimises emergency/disaster management in FM (Arslan *et al.*, 2014). However, a cyber-attack might infringe the integrity and availability of BIM data (Henderson, 2019), leading to a failed management of emergency situations and incurring loss of life and injury for the occupants (Kennett *et al.*, 2005). Furthermore, section 2.3 highlights the importance of data confidentiality, by discussing the impact of a breach in data confidentiality on the organisation and its employees.

The review of BIM benefits in section 2.3.2 also highlights the benefits associated with the process optimisation that is brought to the FM organisations. For instance, accessibility of the updated information of a facility, improves decision making regarding cost estimations and resource allocation, which potentially brings financial gain for the FM organisation (Guillen *et al.*, 2016). However, a malicious unauthorised-access to the FM bidding-documents or contractual agreements might result in legal and reputational implications for the organisation, followed by financial loss (O'Neil and Saleeb, 2019).

Table 2- BIM-FM Cybersecurity Risk Impact

			Violation of Security Triad Impact (Availability, Integrity, Confidentiality)			
	Task Area	**Data in Use**	**Information Availability Loss**	**Information Integrity Loss**	**Information Privacy Violation**	**Resources**
BIM-FM	Asset Management	Personal Identifiable Information, Capital/Operational, Cash flows Cost reporting and Forecasting, Financial Risk Management, Contractual and Legal	Financial Loss, Unavailability of real-time quantity verification resulting inaccurate estimations and forecasting,	Financial loss due to inaccuracy of information Inaccurate and unrealistic visualisation of data for estimation	Reputational Damage Leading to Financial Loss, Intellectual Property Right Breached, Legal and Reputational Implications	(Abdelmohsen *et al.*, 2011; Alkasisbeh and Abudayyeh, 2018; 2012b; Boyes, 2015a; British Institue of Facilities Management, 2012; Ghosh, A., Hosseini, M. R., Edwards, D., Kassem, M., & Matteo-Garcia, 2019; Guillen *et al.*, 2016; Kassem *et al.*, 2015b; Naghshbandi, 2016b; Purpura, 2019; Tang *et al.*, 2020)
	Space Management	Equipment and Furnishing Data, Services and Substructure	Time and Cost consuming processes due to the unavailability of updated information in the right time, Unavailability of data for monitoring and tracking space usage and interiors condition.	Inaccurate safety and Security Measures compromising the safety and security , Modification or falsification of data results inaccurate and wrong decision making leading to cost, time, safety, and security losses, Unavailability of accurate data could incur safety risks as a result of impaired decision making	Financial and Reputational damages due to interception of intellectual property. Unauthorised use and theft of sensitive information could compromise safety and security as well as business continuity.	(AEC (UK) Committee, 2012; ARCHIBUS, 2013; Ashworth, Tucker, Druhmann, *et al.*, 2016; Becerik-Gerber *et al.*, 2012b; IET, 2013; Love *et al.*, 2014; Mayo and Snider, 2016; 2012; Steiner, 2006)
	Operational Management	Building Shell Information, Building Interior	Time and Cost loss to acquire the lost information. Unavailability of real-time data in emergency events incur safety risks. Unavailability of real-time services data in emergency events incur safety and security risks.	Modification or falsification of data results inaccurate and wrong decision making leading to cost, time, safety, and security losses.	Unauthorised use and theft of sensitive information could compromise safety and security as well as business continuity.	(Arslan *et al.*, 2014; Barbarosoglu and Arditi, 2019; Boyes, 2015a; Carnero and Gómez, 2017; Carreira *et al.*, 2018; Chen *et al.*, 2020; Davtalab, 2017; Federal Emergency Management Agency, 2003; Gao and Pishdad-Bozorgi, 2019; Gourlis and Kovacic, 2017; Kassem *et al.*, 2015a; Kennett *et al.*, 2005; Lavy and Jawadekar, 2014; Lee *et al.*, 2013; Mantha *et al.*, 2020; Matarneh *et al.*, 2019; Minoli *et al.*, 2017; Mohanta and Das, 2016; Mutis and Paramashivam, 2019; Naghshbandi, 2016b; Patacas *et al.*, 2015; Pishdad-Bozorgi *et al.*, 2018; Sullivan *et al.*, 2010; Wang *et al.*, 2014; Wu and Issa, 2015; Yam *et al.*, 2001)
		Services Data, Health and Safety Risk Assessment Data, Building Performance Data	Unavailability of real time access to operations, maintenance owner use manuals and equipment specifications. Unavailability of data for monitoring and tracking facility performance and equipment condition data. Time and cost consuming processes of acquiring updated information about the facility. Health and Safety is compromised in emergency events.	Safety and Security infringement due to inaccurate data regarding equipment and condition. Operational disruption leading to charges	Unauthorised use and theft of sensitive information could compromise safety and security. Financial and Reputational damages due to interception of intellectual property.	

Table 2 summarises the findings from sections 2.3 and 2.4 to show the impact of a cybersecurity breach in various task areas of FM. It highlights the threats associated with the infringement of data integrity, availability, and confidentiality across the three main FM task areas of financial asset management, space management, and operations & maintenance. By showcasing the criticality of the impact of cybersecurity risks in FM, it contributes to raising awareness amongst the FM professionals; and justifies the need for a proactive approach towards the development of a strategy for tackling the issue of cybersecurity.

The challenges of BIM in FM, highlighted in section 2.3.3 identified that implementing BIM in FM heightens the cybersecurity risk by creating different vulnerabilities which are people-related (lack of knowledge), process-related (lack of compliance, lack of formal documentation) or technology-related (issue of interoperability, lack of security protection). However, section 2.3 also highlighted that in managing cybersecurity, over-reliance on technical cybersecurity measures overlooks the management of people and process aspects of cybersecurity. Such an approach is regarded as ineffective for the management of cybersecurity in organisations. Therefore, the next section explores how the BIM-FM organisations can minimise their cybersecurity vulnerabilities, taking into consideration the role of people and process.

2.4.4 Cybersecurity of BIM-enabled Facilities Management

Facilities management organisations are responsible for managing and maintaining facilities safely and securely (Glantz *et al.*, 2016). The adoption of BIM in FM and its incorporation with other systems and networks within facilities management forms a bridge between the physical building and its intangible assets. Traditional facilities management focuses on managing the physical aspects of buildings such as fire safety, equipment safety and physical security (Enoma *et al.*, 2009; Leung *et al.*, 2005). However, the security of BIM data and the CDEs supporting digital collaboration in BIM projects are often disregarded and overlooked (Mutis and Paramashivam, 2019). The built environment is not exempt from the eminent threat of cyber-actors and hence, the FM organisations, in particular, the BIM-FM organisations, capable of real time managing of facilities, must incorporate cybersecurity considerations in their work plans (IET, 2013).

Section 2.4 illustrated that a malicious cyber-intrusion is often associated with a physical target and leads to physical harm. The combined physical impacts and cyber-impacts of such attacks

have caused uncertainties regarding the accountability of risks and how they should be managed in FM organisations (Mayo and Snider, 2016). The lack of knowledge and skills in handling and managing digital BIM information amongst the FM professionals, results in poor cybersecurity practices when exchanging and storing digital BIM data, leading to an increased vulnerability of their systems to such attacks. This is mainly due to the lack of cybersecure interaction with BIM infrastructure and tools (Boyes, 2015a).

Cybersecurity threat to BIM-enabled facilities management is heightened by the digital collaborations brought by BIM, where the impact of a cybersecurity attack is heightened due to the existing connection with building management systems (BMS) (Mayo and Snider, 2016; Minoli *et al.*, 2017). An attack to the CDE can act as a vector of attack to the FM control-systems and enable unauthorised access to systems leading to disastrous outcomes for the facility and occupants. This may cause disruption to services, or result in a loss of control, leading to serious health and safety harm to the occupants, such as the disabling of fire alarms which could pose life threatening implications in a fire incident. (Boyes, 2015a; Purpura, 2019). The scenario is exacerbated in the case of highly-intelligent buildings with multiple interconnected IoT devices that are operating through digital networks (Mantha and de Soto, 2019).

An attack to the BIM can act as a vector of attack to the FM control systems; to exemplify, access to BIM data can expose details of CCTV specifications and locations, easing the way for potential threats, such as theft, terrorism, and unauthorised access to the building (Boyes, 2015b). Furthermore, a vector attack to a CDE may lead to access to control systems. In the example of CCTVs, a malicious cyber-intrusion could lead to the loss of data availability by deleting the CCTV footage, or compromising information confidentiality by allowing the unauthorised viewing of images, or tampering and altering images to compromise the information integrity (Abie, 2019; Boyes, 2015c).

Thus, the implications of cyber-attacks and their impact on the tangible and intangible assets of a facility need to be understood by the FM team. However, the multi-faceted nature of the problem does not match the existing competencies of the FM organisations (De Soto and Karri, 2020) . Hence, it is important to investigate the impact of cyber threats on buildings, to provide an insight into the cost of a cybersecurity attack in various FM task areas, and the way it compromises the benefits associated with the adoption of BIM in FM. This will establish the

importance of understanding, managing and preventing cybersecurity risks in BIM-FM (Mantha *et al.*, 2020).

2.5 Cybersecure management of BIM in FM

The review of literature highlighted that the challenges and shortfalls associated with the implementation of BIM in FM contribute to more cybersecurity vulnerabilities, therefore it is concluded that cybersecurity considerations should be integrated within the implementation and management of BIM. To overcome the challenges associated with the implementation of BIM, maturity models are developed to assist organisations in assessing and evaluating their capabilities with respect to the competencies set out in the model (Mom and Hsieh, 2012). Hence, this study explores the BIM-maturity models to identify the determinants that contribute towards a cybersecure BIM-FM organisation, to help overcome the vulnerabilities discussed above.

'Determinant' is a term commonly used to address the influential factors that are believed to affect or have empirically demonstrated to affect the outcome of an application (Nilsen, 2015). Proctor et al., (2011) discuss the variety of terms used interchangeably with 'determinants', such as challenges, hinderers, enablers, impediments, and many other similar terms amongst academia. Proctor et al., (2011) further emphasise the variety of terms accounting for the "application outcome", such as adoption, compliance, behaviours, use and uptake of a concept or practice, which are influenced by determinants. The extraction of determinants is achieved by reviewing the competencies required, at the highest level of maturity, in BIM maturity models that are applicable to FM organisations. The selection is also focused on the socio-technical aspects of BIM, in line with the focus of this research.

2.5.1 BIM Maturity Models

Various definitions of maturity are proposed by researcher studies. Azzouz *et al.*, (2016) suggests maturity is the state of full development or development that has reached its optimal state. Fahrenkrog *et al.*, (2003) proposed a similar definition of maturity as defining, managing, measuring, or controlling a specific process, by which the consistency and capabilities of the organisations for managing its projects can be indicated. In line with this, Cooke-Davies, (2004) points to organisational maturity which defines the ability of an organisation to deploy a certain process, through the use of process documentation, management, measurement, control and continuous improvement. Schumacher *et al.*, (2016) also refers to the

organisational maturity as the organisational improvement and advancement of processes over a certain period of time. Process maturity is commonly used to describe how productivity and quality can be improved in an organisation through consistent and efficient processes (Almarabeh and AbuAli, 2010; Khoshgoftar and Osman, 2009; Paulk, 1995). As such, organisation maturity is led by its ability to perform certain processes in a well-defined manner with clear roles and responsibilities (Khoshgoftar and Osman, 2009). Achieving a higher level of maturity is likely to result in greater chances of success in projects (Vaidyanathan and Howell, 2007).

There are various BIM maturity models developed across the globe, which can be utilised by organisations and industry practitioners (Chen and Luo, 2014; Giel and Issa, 2013; Mom and Hsieh, 2012; Succar, 2010). Existing maturity models are focused on a variety of BIM capabilities, including the various applications of BIM (e.g.4D, 5D), BIM modelling, organisational readiness, maturity of BIM processes and procedures, and technological facilities (Chen and Kamara, 2011; Giel and Issa, 2013; Mom and Hsieh, 2012; Succar, 2010).

Continuous assessment of BIM maturity in organisations assists them with the setting of achievable goals that will eventually lead to the highest-level of BIM maturity within an organisation (Lockamy and McCormack, 2004; McCormack *et al.*, 2008). By structuring and categorising various aspects of BIM, maturity models assist organisations to make changes to one aspect at a time. This enables better monitoring and management of improvements and changes and allows for an optimum approach towards reaching the higher levels of BIM maturity (Cooke-Davies, 2004; Khoshgoftar and Osman, 2009). Hence, BIM maturity can be considered as the ability to execute BIM repeatedly with a certain degree of quality (Succar, 2010). In order to achieve maximum benefits from BIM, users must achieve BIM competencies to the level that determines a mature implementation of BIM in an organisation (Giel and Issa, 2013). A mature implementation of BIM translates into an improved quality of service and enhanced collaboration and coordination amongst those involved (Giel and Issa, 2013; Nepal *et al.*, 2014; Succar, 2010), therefore, reducing the challenges and shortfalls which create cybersecurity vulnerabilities in BIM-FM (see sections 2.3.3.1).

Various organisational maturity models to identify the BIM determinants which contribute to a more cybersecure BIM in FM are reviewed below. The focus area of each model is presented in Table 3 to enable better comparison:

- The NBIMS Capability Maturity Model was developed by the National Institute of Building Science in 2012. The model is used to evaluate implementation of BIM in 11 areas, while using it on a 10 level scale (NIBS, 2015). A final score is calculated using weighted scoring methods for all the 11 areas which are then mapped to the five-grade scale of the maturity model, where the lower level is level 1, indicating initial improvement and the highest level is level 5, indicating continuous improvement (Maradza *et al.*, 2013). This model is focused on the data and modelling capabilities, including interoperability, precision, and richness of information, as well as the graphical and spatial capabilities of the data, throughout the BIM lifecycle. Hence, it can be used by all stakeholders involved in a BIM project (McCuen *et al.*, 2012). This model has been criticised for lack of clear definitions for the maturity determinants which has resulted inaccurate maturity rating, due to various interpretations by the maturity evaluators (Kassem and Li, 2020).
- The Construction Industry Council (CIC) was developed as a BIM planning guide for facility owners-version 2.0, in 2013, which was accompanied by an owner BIM matrix which is considered to be amongst the most effective BIM maturity models, due to its specific focus on FM organisations and its clear description of evaluation methodology (Construction Industry Council, 2013). This was later updated in 2018 as part of CIC's efforts in addressing the most recent demands of the industry. In this guide, the planning phase is focused on the needs of facility owners by understanding their information requirements and goals (Dakhil *et al.*, 2019) The guide comprises of 6 key elements that help in planning BIM implementation (Kassem and Li, 2020) :
    - Element 1- Strategy: Identifies strategic aspects such as goal, vision, mission, and objectives from which the purpose of adopting BIM can be determined.
    - Element 2- Implementation: Discusses the methods and stages of BIM implementation; including generation, processing, communicating, executing, and managing.
    - Element 3- Process: Describes the means of implementing BIM which could be continuous, or transitional.
    - Element 4- Information: Facility data such as the level of details, data, and model breakdown.
    - Element 5- Infrastructure: The medium needed for BIM implementation such as software, hardware, or physical space.
    - Element 6- Employee: Capabilities, roles and responsibilities, training requirements, change management and education are all part of it.

The model has adopted a holistic approach towards evaluating maturity in FM/owner's organisations, where the people and processes of BIM implementation are taken into account.

- The Owner's BIMCAT is another model that is used to evaluate maturity of BIM in owner organisations (Wu *et al.*, 2017). This model is an extensive evaluation tool covering every aspect throughout the lifecycle of the asset (Azzouz *et al.*, 2016). This maturity model is divided into operational, strategic, and administrative competencies, where the main focus is on the operational considerations pertaining to the quality of information (data richness, geometry, technology, etc.). The user can evaluate the BIM deliverables and define the requirements with respect to the extent that the organisation uses BIM in its projects. The strategic competencies relate to documentation, project standards and goals. The model also focuses on administrative competencies including project procedures, polices and cultural aspects, as well as the operational considerations (Giel and Issa, 2013). The model is more comprehensive when compared to others, as it assimilates competencies from the literature and a number of existing models such as NBIMS and BIM Maturity Matrix. However, this model has been criticised by the clients, for its complexity of use in comparison to the five level models (Wu *et al.*, 2017). Also, the justification of the selected methodology for the development of this model was found to be vague (Giel and Issa, 2013; Kassem and Li, 2020).
- The Netherland's Organisation for Applied Scientific Research (TNO) developed a maturity model called TNO's BIM Quick Scan in 2012, which was superseded by BIM Compass in 2019 (Kassem and Li, 2020). BIM Compass was developed for all organisations who intend to adopt BIM, with particular focus on the design, engineering, and construction firms. Organisation and management, cultural aspects, information structure and flow, and tools and applications were the four criteria that were included in this model. The evaluation process addresses ten aspects that include strategy, organisation, resources, partners, mentality, culture, education, information flow, standards, and tools (Sebastian and Van Berlo, 2010). This tool is not applicable for small and medium organisations and is more targeted towards the pre-built phases of a BIM project (Van Berlo and Hendriks, 2012; Kassem *et al.*, 2013).
- The Indiana University's BIM Proficiency Matrix was developed in 2009. This model was mainly focused on both the designer and contractor competencies in BIM, where all categories were allocated the same weight (Dakhil *et al.*, 2019) .A score between zero and

one is given for each category with zero indicating that this element is not existing and one indicating a fully-functional element in the model (Indiana University, 2009). The model was criticised for being subjective with limited technical-evaluation capabilities and its inconsistencies that make it unreliable in many cases (Succar, 2009). These limitations were overcome by the Succar Maturity Model in 2009 which provided comprehensive explanations for each category, from which the inconsistences were minimised and more attention was given to socio-technical aspects (Giel and Issa, 2013; Succar, 2010).

- One of the highest-rated efforts in the development of maturity models was the work of Succar in 2009, which took into account all aspects of technology, process and policy (Kassem and Li, 2020; Succar, 2015). This five-point scaled evaluation-model can be used by different types of organisations. The model comprised BIM-capability sets, BIM-maturity index, BIM-capability stage, and organisational scale. These components were linked to form the BIM maturity matrix. The model offers a distinction between BIM capability and maturity inside an organisation and the BIM capability stages (Kassem and Li, 2020; Succar *et al.*, 2013). In this model the capability is defined in the model as the ability to deliver a certain service or product while maturity is related to the quality of delivering and executing a service (Giel and Issa, 2013). The model was based on a combination of NBIMS and CMM, which narrows the gaps between process, policy, and technology. The model is one of very few that indicate the management of data access and information security in BIM-enabled organisations (Li *et al.*, 2017). The model later contributed to the BIM Excellence online platform by Change Agents (AEC) in Australia (Kassem and Li, 2020).
- The UK BIM maturity model was developed in 2008 by Bew and Richards (Bew, M., and Richards, 2008). This model was considered as the main component in the strategy adopted by the UK for BIM implementation, however, it serves as a capability model that is used as the base of a number of BIM maturity models that were later developed (Succar, 2015). BIM Compass is one of the models that uses the Bew Richards BIM maturity model to plot the scores (Kassem and Li, 2020).
- The Vico BIM Scorecard was developed by Vico Software in 2011, to assess the use of BIM in the day to day tasks within the general contractor organisations (Kassem and Li, 2020). This model is mainly focused on product and cost control as well as some organisational process-related capabilities (Giel and Issa, 2013).

- The Construction Project Information Committee developed a BIM assessment form (CPIx BIM-Assessment) in 2011, with the aim of evaluating the maturity of BIM in supply chain organisations and consultancies. Therefore, its main focus is on the understanding and capabilities of the organisation in modelling, planning and operating BIM, with minimal focus on the people and process aspects of BIM implementation (Kassem and Li, 2020).
- The National Federation of Builders (NFB) developed an online assessment of BIM maturity to evaluate the competency and readiness of organisations to improve the maturity of their BIM implementation. It includes consideration for both people and processes regarding digital collaboration in BIM-enabled organisations.
- Constructing Excellence (hosted by Scottish Futures Trust) developed a compliance-evaluation tool that assesses the maturity of BIM adoption, based on the level of compliance against levels 1 and 2 BIM in the UK (Kassem and Li, 2020). The results of the evaluation provides a grade to show where the organisation stands with respect to the industry standards of level 1 and 2 BIM (Kassem and Li, 2020).
- The VDC Scorecard was developed in 2012 by Stanford University (Calvin Kam *et al.*, 2013). The intent of this model was to conduct a comprehensive adaptive assessment that was practical and flexible to the users (Calvin Kam *et al.*, 2013; Kam *et al.*, 2014). The model was mainly intended to assess BIM maturity in projects, but it also includes organisational readiness competencies. The user can analyse input data when using VDC Scorecard and assess whether they comply with the pre-set objective. However, its credibility has been largely subject to criticism, due to the small number of case studies used in the development of the model (Azzouz *et al.*, 2016).

Table 3- BIM Maturity Models Evaluation Focus

Framework/Authors	Core Focus	Applicable Stakeholders
NBIMS-CMM (NIBS, 2007) Interactive Capability Maturity Model	Data generation and delivery (graphical, spatial capabilities, interoperability, delivery method, etc). Processes and procedures Roles & Responsibilities	Architecture Engineering Construction FM/Owner
Succar's BIM Maturity Model (Succar, 2009) as part of BIMexellence	Focused on People, Policy, Technology Collaboration processes among multiple departments or external stakeholders Information management strategies Alignment of BIM implementation techniques with strategies (goals at organisational level) BIM supporting infrastructure (hardware, software, network) BIM management and leadership Organisational BIM responsibility hierarchy Employee performance in BIM implementation	Design Construction Operations & Maintenance (FM)

	and execution Development of BIM formal documentations and contracts Compliance and quality control plans	
BIM COMPASS (Replaced TNO's BIM Quick Scan, Sebastian & Berlo, 2010)	Organisational Management Technical & Modelling Cultural considerations and employee performance	All stakeholders
Scottish Futures Trust BIM Compass	Compliance with level 2 standards (some of which are now superseded by ISO19650: 1. Collaborative Management: BS1192:2007 2. Design Management: BS7000-4:2013 3. Library Objects: BS8541 4. Information Management (CAPEX): PAS1192-2:2014 5. Information Management (OPEX): PAS1192-3:2014 6. Information Exchange: BS1192-4 7. Soft Landings: BS8536 8. Security: PAS1192-5	Applicable to procurers and suppliers in all phases of a BIM project.
BIM Proficiency Matrix (Indiana University 2009)	BIM execution plan (BEP) standard BIM-enabled project delivery methods and deliverables requirements Planning, design, construction, operation phase uses Asset management, space management, design/programming, construction cost data Design, construction, as-built model geometry Design collision detection, construction clash detection	For Owner's/FM's use to assess maturity of designers and contractors
CIC Research Program's BIM Maturity Matrix (2012) CIC BIM Protocol (2018)	Purpose of BIM implementation (goals, vision, mission, objectives) Method of BIM implementation (generating, processing, communicating, executing , managing) Means of BIM implementation (current ,target , transition) Information requirements of the facility (model element breakdown, level of details ,etc) Infrastructure required to support BIM implementation(software, hardware , workspace) People (responsibilities, hierarchy , education, change readiness)	Owners/FM
Owner's BIMCAT (Giel and Issa 2013)	Modelling capabilities Technology Infrastructure Data quality Strategies Managerial plans	Owners (Possibly FM)
UK BIM Maturity Matrix (Alliance for Construction Excellence 2008)	Focused on modelling capabilities and data handling, Compliance to standards and guidelines	Generic
NFB Online BIM Maturity Assessment	Strategy Knowledge & skills Information management processes Technology Excellence Modelling and technical considerations	Generic

CPIx BIM Assessment Form	Modelling and technical capabilities	Supply-chain Consultants
Vico BIM Scorecard	Organisational BIM processes Project specific capabilities Modelling and technical considerations	General Contractors (mainly pre-construction)
VDC BIM Scorecard (KAM 2013)	Alignment of project goals with organisational objectives (planning) Organisational BIM processes (adoption) Technical modelling and data-related considerations (technology) Project Performance	Generic (for all AECO stakeholders to assess their organisational readiness along with project maturity)

2.5.1.1 Selection of maturity model

The maturity models intended for assessing organisational BIM maturity were investigated for their applicability to the facilities management organisations and their focus on the aspects of BIM which were related to people and processes. Particular attention was given to the models that refer to the management of BIM data security from a non-technical perspective, however, data security was either overlooked across most models, or considered as part of the technical and technological considerations. Although several models were identified as applicable to the FM organisations, not all of them focus on BIM maturity in FM organisations, in relation to people and processes. Models such as the VDC scorecard, CIC BIM Maturity matrix, BIM compass, Scottish Futures Trust BIM compass, the Succar BIM Maturity matrix and BIM Compass (Netherland) all include people and process aspects of BIM maturity in organisations and target the FM organisations, as their users (Azzouz *et al.*, 2016; Kassem and Li, 2020; Wu *et al.*, 2017). However, many of them have limitations in terms of people and processes aspects that they focus on. To exemplify, the VDC scorecard is mainly focused on project maturity in BIM organisations, however, it also includes organisational readiness capabilities as part of its assessment (Dakhil, 2017). The Scottish Futures Trust BIM compass is mainly based on the organisation compliance to standards and guidelines, where it is assumed that compliance guarantees maturity, and overlooks considerations related to people and processes to achieve compliance. Furthermore, although Netherland's BIM compass includes considerations for people and processes, it mainly encompasses modelling and technical capabilities (Kassem and Li, 2020). The NFB online BIM maturity assessment includes some consideration for people and processes which include information management processes, training and education, and strategy, however, it does not include many additional factors, unlike both the Succar maturity-model and CIC BIM-maturity matrix which include quality assessment, cultural considerations, and risk management.

The maturity models of both Succar and CIC focus on aspects of BIM maturity in organisations that relate to people and processes as well as technical and policy considerations. (Azzouz *et al.*, 2016; Dakhil *et al.*, 2019). These two models did not align with any particular BIM standard to develop their models, therefore, the generic nature of these models increased their applicability to the FM organisations, as well as allowing for an integration of their proposed determinants with cybersecurity determinants. Also, both the Succar and CIC models have been found more credible for providing a detailed explanations of the assessment philosophy and methodology, to provide a holistic understanding of BIM competencies and maturity levels (Dakhil *et al.*, 2019; Kassem and Li, 2020).

2.5.1.2 BIM-FM Determinants

The maturity models of both Succar and CIC were chosen to be studied for the identification of determinants applicable to BIM-FM that contribute to minimising the cybersecurity vulnerabilities arising from the challenges of BIM implementation in FM. The selection of determinants was based on the following defined set of criteria:

- As this research was focused on people and process considerations for improving the cybersecurity of BIM-enabled FM organisations , determinants pertaining to technical and technological aspects of BIM were ruled out in the selection.
- The applicability of determinants to the facilities management organisations was derived from the literature review in the domains of BIM-enabled FM, BIM benefits in FM and BIM challenges in FM.

The determinants were identified from the review of both the Succar and CIC maturity models and presented in the following section. The following references were used in writing the description of each determinant (Chunduri *et al.*, 2013; CIC, 2013; Giel and Issa, 2013; Isikdag, 2012; Kassem and Li, 2020; Kelly *et al.*, 2013a; Succar, 2010).

2.5.1.2.1 Purpose of BIM Implementation (Goals, Vision, Objectives)

Strategic considerations including goals, vision, and objectives to portray the purpose of BIM implementation in an organisation were indicated by many of the maturity models, including the Succar and CIC models, together with the Netherland BIM-Compass and NFB Maturity-Assessment. The importance of visioning what the organisation was striving to accomplish has been emphasised in achieving a mature implementation of BIM. In the CIC model, goals, visions, and objectives lead the organisation towards reaching its optimum purpose. Hence, in a facilities management organisation, a transformation from the traditional ways of working,

to the BIM-enabled ways of working, requires a clear purpose, that sets the direction and acts as a reference goal. The purpose of BIM implementation within an FM organisation would be the benefits of BIM within FM. According to the Succar BIM maturity model, the strategic planning of BIM mission, vision and objectives should be created by the management of an organisation and should set the scene for all operational teams. A clear purpose would affect the performance at all levels, and when well-integrated within all strategic plans, would stream-down through the implementation processes.

2.5.1.2.2 Infrastructure required to support BIM implementation (Software, Hardware, Network)

Many maturity models have addressed the importance of investment in advanced BIM infrastructure, including software, hardware, and networking systems, and some have also focused on competencies that are more inclined towards the managerial efforts that lead to technological excellence. The CIC model describes infrastructure maturity as the availability of updated software and hardware that is capable of undertaking BIM operations and modelling. The Succar model has expanded the scope of infrastructure maturity, by also taking into account the strategic and implementational considerations required, to manage and maintain technological excellence in a mature implementation of BIM. It describes the optimum state of infrastructure maturity as the availability of a strategic plan to continuously monitor, control, update and improve the functionality, deliverables, and communication processes. It also refers to the data interoperability considerations as well as regulating communications and exchange of data, in line with organisational strategies. The compatibility between the degree of technological advancement and strategies in place is emphasised by the Succar model. Hence, considerations for implementing the required BIM infrastructure should encompass foundational strategies that can support the uptake of advanced BIM technologies.

2.5.1.2.3 Interaction Co-ordination and Communication Processes with contractors and sub-contractors

This determinant is indicated in a number of the maturity models including the NFB online maturity assessment, CPIx BIM assessment form, and the Succar and CIC models. However, each maturity model had its own unique lens for assessing the maturity of this determinant. Whilst Succar's model was more inclined towards the operational and technical aspects of stakeholder interaction, collaboration and communication, the CIC model emphasised the documentation of BIM processes, both at the organisation and project level. This pertained to

the development of documents such as the BIM execution plan (BEP) and general procedures related to BIM works, to improve the management of internal and external communication processes. The CIC model was the only one which specifically targeted the development of plans that led to the accomplishment of implementation goals. Hence, it considers the objectives and potential benefits, that are achievable through the interaction, coordination, and communications processes with reference to the strategic goals.

2.5.1.2.4 Competent BIM Implementation Management

A competent and mature approach towards managing BIM implementation in projects has been addressed by many maturity models, each through a different lens. Each model has indicated a number of factors that this competency entails. CIC maturity matrix refers to the management of BIM implementation in terms of the project uses and organisational operations. The first factor pertains to the extent of BIM use in projects and the extent of digital collaboration associated with the projects. The second factor pertains to the extent of BIM integration with the daily operational tasks of an organisation. For the CIC model, the availability of data in real-time and the information use during the lifecycle of a project was deemed crucial for competent implementation-management in BIM projects. The Succar model, on the other hand, focuses on the quality of data exchange and the information loss within the transitions. It also focuses on the compatibility of the implementation management with the organisational strategy. Both CIC and Succar's models have focused on the development of information requirements, BIM execution plans (BEP) to document processes, and contracts specifying information need and model structure, to ensure a competent management of BIM implementation in the operations of the organisation.

2.5.1.2.5 Arrangement of BIM Duties and Roles

Arranging the roles and responsibilities within a BIM-enabled organisation is pointed out by the majority of the maturity models, including Netherland's BIM compass, NBIMS capability Succar's maturity matrix and CIC BIM maturity matrix. In a BIM-enabled organization, BIM roles and responsibilities are incorporated within the job descriptions. Roles are the functional duties that the employees are required to carry out. Each BIM role is assigned one or multiple obligations which are labelled as BIM responsibilities. The CIC and Succar models have both addressed the importance of having an organisational hierarchy of BIM roles and responsibilities to ensure a smooth flow of BIM processes and procedures. Both models have also indicated that defining BIM roles and responsibilities should be followed by ensuring that

those assigned have sufficient capabilities to undertake their responsibilities. It is further pointed out that defining roles and responsibilities enable the identification of suitable training and education for employees. The Succar model further emphasises that an optimised maturity in BIM entails BIM roles and duties that are continuously assessed to ensure employees can fulfil the organisational BIM process requirements.

2.5.1.2.6 BIM Knowledge and Skills

BIM knowledge and skills were included within many of the maturity models, from both the operational and managerial aspects. Netherland's BIM Compass and the VDC scorecard were focused on the need for both technical and modelling skills for a BIM-enabled project, while other models such as Succar and CIC also indicated knowledge management being a requirement depending on the roles and responsibilities of employees. Furthermore, the two models also take into account the BIM leadership and management capabilities with respect to the extent of their support as well as the employee awareness and readiness to take on the digital shift brought by BIM.

2.5.1.2.7 Compliance with BIM Standards and Guidelines

The Succar, CIC, and Owner's BIM CAT models have the highest focus on compliance measures contributing to the maturity of BIM within an organisation. The Succar model considers the adherence of contractual agreements regarding BIM processes and procedures, risk management, and the delivery of project deliverables important, whilst the CIC model has indicated the importance of developing BIM documentation in compliance with best practice guidelines and standards and using the standard document templates (e.g., BEP templates). The CIC model further takes into consideration the compliance of information sharing regulations, information requirements and the structure of the model with best-practice guidelines and standards.

2.5.1.2.8 Quality Control Plans

Quality control was considered an important determinant for a mature adoption of BIM within an organisation. The Succar maturity matrix, Netherland's BIM Compass and NBIMS have all included this determinant as a competency that should be measured. However, the focus is commonly shifted towards the quality of deliverables rather than process benchmarking. Although the Succar model considers monitoring, revising, and improving the various competencies to the optimum maturity level, to ensure the processes and procedures of BIM implementation are in line with the strategic goals and objectives of the organisation.

2.5.2 Cybersecurity Considerations in BIM-FM

The review of BIM maturity models illustrated a lack of focus on the issue of cybersecurity in BIM-enabled FM. The existing maturity models tend to point to the management of both information and communications, together with cybersecurity considerations as part of the infrastructure maturity (section 2.5.1.2.2). This implies a technical view of the issue of cybersecurity in BM-FM, and does not consider the effects of strategies, processes, and people. This also results in an isolated approach, where only those involved with the IT and infrastructure are responsible for managing and maintaining cybersecurity. Section 2.4 emphasised the importance of considering both people and processes aspects of managing cybersecurity, as well as technical considerations. Therefore, this research proposes the integration of cybersecurity in strategies, processes, and performance, to ensure a cybersecure implementation of BIM in FM.

Therefore, to bridge the gap between the BIM and IT in FM, this section seeks to identify the cybersecurity determinants which can be integrated with the BIM-FM determinants identified in section 2.5.1.2. This approach is in line with the study of Dourish and Anderson, (2006) who propose a holistic approach towards the issue of cybersecurity within organisations, by incorporating secure intra-organisational and extra-organisational collaboration methods, regulations and policies, and technologies in a unified strategy. A cybersecurity-minded working strategy within an organisation, results in a proactive approach towards assuring the confidentiality, integrity and availability of digital information and optimum resilience against malicious cyber-activities (Baskerville and Siponen, 2002). Hence, the integration of cybersecurity determinants with BIM-FM determinants enables a unified approach towards the management of cybersecurity, as part of managing BIM in FM organisations.

2.5.2.1 Cybersecurity Management Guidelines and Resources

There are standards, best practice guidelines, frameworks and models developed by the regulatory bodies and academics to assist organisations to achieve cybersecurity within their working processes.

Academic contributions towards producing models that assist organisations in a better cybersecurity management, differ in both approach and perspective. To exemplify, the Gerber and Von Solms (2005) approach is criticised for overlooking people, process and policies and for limiting their focus to the cybersecurity of systems. Alternatively, Da Veiga and Eloff,

(2007) offer a view that is inclusive of the effects of people, process and technology on the cybersecurity of an organisation. The various viewpoints can be perplexing to organisations who wish to select the most compatible approach for incorporating cybersecurity best practices within their business processes (Paulsen, 2016). However, it can also complicate the adoption of a strategic approach within organisations who are at the early stages of improving cybersecurity (Minoli *et al.*, 2017; Toth, 2016).

Standards and best practice guidelines developed by the regulatory bodies also offer various viewpoints on the issue of cybersecurity by focusing on technology, process, people and policies (Bayuk, 2012; Wang *et al.*, 2015). In effect, standards direct organisations to optimise cybersecurity, by improving their structure, processes, plans and culture (BSI, 2007). As organisational cybersecurity is rooted in its information security foundations, various resources are available to assist organisations in defining and developing their cybersecurity strategy in line with their business framework (Brackney and Anderson, 2004; Sallos *et al.*, 2019). Some of the most commonly used standards and procedures include ISO27001, COBIT, ISO 20000, ISO 38500 , ISO 17 799, NIST Special publication 800-160, BS1192:5, PAS 555:2013, IASME (Ula, Ismail and Sidek, 2011; BSI, 2012). ISO 27001 and COBIT 5, have integrated the technological aspects of cybersecurity with the key aspects of cybersecurity management, taking into account people, process, and policies (Information security forum, 2005; ISACA, 2012a). These are further explored below:

- COBIT: The primary efforts of ISACA (Information Systems Audit and Control Association) towards the development of COBIT 5 resulted in a framework with a focus on aligning IT and business strategies. The framework was further revised in 2003 to deliver a unified approach towards the management of cybersecurity risks, as part of a unified risk-management. COBIT 5 considers all levels of management, operations, and executive business units to contribute to the development of a cybersecure organisation. It further accentuates the roles of stakeholders and governing bodies on the quality of cybersecurity implementation within an organisation. Its main focus is on the management and monitoring of principles, processes, and policies at all levels within an organisation (ISACA ,2012). COBIT 5 encompasses factors that determine the cybersecurity stance of an organisation, including cybersecurity goals, principles, organisational hierarchy for information security, processes and procedures (Bin-Abbas and Bakry, 2014).

- ISO Series: This is an international source of guidance on the management of cybersecurity primarily developed as BS7799. The ISO series includes a wide range of standards for managing different aspects of cybersecurity such as the information-security management system (ISMS) addressed by a sub-division of ISO, labelled as ISO/IEC 27000:2016,2017. This standard offers a systemic approach towards the management of cyber-risk (BSI, 2016). For organisations taking their first steps towards establishing a cybersecurity-oriented structure, ISO/IEC 27001 contains the baseline requirements for the management and maintenance of cybersecurity, whilst BS ISO/IEC 27002 offer further details on other aspects including processes and procedures, technology enablement, rules and regulations, and roles and responsibilities. As per BSI, (2012), alternative ISO standards including ISO/IEC 27005:2011, 2018 and ISO/ICE 27032:2012 are efforts towards preparing organisations to adopt a cybersecure approach within their everyday job tasks. The ISO series are well-recognised around the world and particularly in the UK, and they remain as traditional guidelines for the management of cybersecurity within organisations (Culot *et al.*, 2019). Their limited indication towards the interactions of people and technology is usually criticised by those who believe the ISO series are overly restricted to the cybersecurity of systems (Nye, 2018).
- NIST special publication 800-100:This standard proposes the integration of cybersecurity within organisational policies and accentuates the importance of having the commitment and push from the management team to accommodate suitable cybersecurity training for employees, and the allocation of sufficient resources to support the integration (Bowen *et al.*, 2006; Paulsen, C. Toth, 2016). As per Bowen *et al.* (2006), factors such as a competent security team, development of a cybersecurity-oriented organisational structure, and effective monitoring and auditing are proposed by NIST. Thomborson (2010) also encourages investigating the cybersecurity requirements of the organisation, to achieve an understanding of the resources required to support the full integration of cybersecurity measures. It proposes a qualitative, rather descriptive modelling of requirements, which elicits cybersecurity requirements by taking into account the protection, and prevention systems to deal with cyber-attack with all their corresponding actors. The cybersecurity-requirement model is then used by the senior-management team to make cybersecurity-aware decisions on budget allocations, organisational structure, and strategic plans.

- NIST RISK MANAGEMENT FRAMEWORK: In an effort to develop a comprehensive, yet detailed solution for risk management, the NIST Risk Management Framework was published in 2014 to manage risks to critical infrastructure (NIST, 2014). It covers all aspects of risk management, including identification, protection, detection, response, and recovery. However, it is criticised for overlooking unknown and unwanted risks, which are commonly known as unpredictable attacks (Hutchins *et al.*, 2015; Task Force Transformation Initiative, 2015). Hence, it does not provide guaranteed resiliency to the evolving nature of cyber-attacks in the world today.
- IASME: ISO, NIST and COBIT 5 are not compatible with all sizes of organisations. IASME (Information Assurance for Small and Medium Enterprises) plays an important role in ensuring the resilience of small and medium sized organisations, in maintaining the confidentiality, integrity and availability (CIA) of information and reducing the impact of a potential attack on both cyber and physical assets (NIST, 2003). IASME is an attempt to support compliance with ISO 27001 to enhance and improve information security within small and medium sized organisations (Clarke, 2015).
- PAS555:2013: As part of the efforts of the British Standards Institute (BSI) to address organisational cybersecurity management, the publicly available specification PAS 555:2013, is another popular source of guidance for the implementation of a cybersecurity-oriented strategy within organisations. It addresses the strategic, operational and technical aspects of cybersecurity integration by accentuating the need to assess the stakeholder cybersecurity-posture to enable successful integration of cybersecurity at the operational level (BSI, 2013b).
- NCSC Cybersecurity Guideline: To promote the development of a cybersecure culture within organisations, the NCSC document "10 steps to cybersecurity" assists them to improve on the existing knowledge, skills and level of awareness which would lead to an improved security posture (NCSC, 2018) .

The review of the available guidelines and standards showed the variety of focus and approach to organisational management of cybersecurity, therefore, none of them could be adopted in isolation, for a comprehensive and inclusive integration of cybersecurity within an organisational context (Tropina, 2020). However, a number of frameworks and models attempt to bridge and unify some of the guidelines, by offering more inclusive guidance that covers

previous published materials and overcomes some of the conflicting instructions by proposing a unified approach.

For instance, the HMG Information-Security Policy Framework and the CESG Cybersecurity model are amongst the frameworks that are built upon the previous efforts in the area of information security and cybersecurity. The CESG cybersecurity model covers the IAMM (Information Assurance Maturity Model) and IAAF (Information Assurance Framework) and is in full alignment with the Luftman (2000) model for evaluating the organisational information-security maturity levels. Furthermore, it complies with the BS ISO/IEC 27001:2005 risk-management principles and BS ISO/IEC 27001 information-assurance principles. The CESG provides a more comprehensive and inclusive oversight into the regulatory principles of information security and in particular cybersecurity management within organisations.

In the context of BIM within the AECO industry, there are no FM-specific guidelines for the cybersecurity management of BIM-enabled working processes and procedures. The PAS1192-5 recently replaced by ISO19650-5 was among the first efforts for addressing the issue of cybersecurity in BIM. This publicly-available specification portrays a cybersecurity minded BIM organisation, which is far from the current stance of BIM-FM organisations (Patacas *et al.*, 2015). Yet, there are no standards or guidelines to address cybersecurity in FM organisations. Therefore, the next section explores cybersecurity determinants that can be integrated with BIM determinants to improve the cybersecurity of BIM-FM.

2.5.2.2 Cybersecurity Determinants

Many resources have considered distinct categories for the factors affecting cybersecurity management within an organisation. To exemplify, Evans and Reeder (2010) highlight factors such as training, culture, and strategy development as internal factors, whilst regulations and stakeholder requirements are deemed as external factors. In line with this, Dzazali and Hussein Zolait (2012) suggest that the interchangeable effects of the internal and external categories unify the factors in such a way that both categories can be developed to address the other. Furthermore, Sommer and Brown, (2011), suggest that the management of cybersecurity is directly influenced by external factors such as regulations and orders, and directed by the intra-organisational factors such as compliance, monitoring and auditing. Therefore, compliance with standards and guidelines should be accompanied by specific determinants to enable the fulfilment of the requirements set out in the best practice documents (Azzouz *et al.*, 2016;

Dakhil *et al.*, 2019; Patacas *et al.*, 2015). A selection of determinants that contribute to an improved cybersecurity in organisations is presented below. Technical determinants were ruled out to maintain the focus of the research on the people and process aspects of cybersecurity. A number of peer reviewed journals in the organisational cybersecurity-management domain and the standards and best practice guidelines reviewed in section 2.5.2.1 were used as resources.

2.5.2.2.1 Systems Security Design

Systems security design is a determinant which has the focus of many cybersecurity specialists within the industry and academia (Butcher, 2019; Gerber and Von Solms, 2005; Mayo and Snider, 2016; Von Solms and Van Niekerk, 2013; Wood, 2000). An effective design of security for information systems requires regular updates to keep up with the ever-growing capabilities of hackers and malicious cyber-intruders (Srinivas *et al.*, 2019). It has also been discussed that a silo approach to cybersecurity, stems from an over-reliance on security systems and technical cybersecurity-solutions protecting systems security. Hence, the approach of Gerber and Von Solms (2005) is criticised for overlooking the important aspects of cybersecurity that entail people and processes, whilst over-focusing on technological aspects. In the light of this, the requirements and regulations of SSE CMM (2003) and ISO/IEC27010 (2012) have insisted on employing the effective management of knowledge, human resources and risk to design, manage and maintain cybersecurity systems with respect to the requirements and regulations. The attempt by the Information Systems Security Association (2004) to identify, assess, manage, and mitigate the cyber-risks to information systems has also focused on an IT-centric framework. Although such an approach can face criticism for its technological fundamentals, it can be of merit when supported by transparent processes and analysis rationale. The attempt by the Cobit 5 framework (ISACA, 2003) to address IT-centric cybersecurity systems and solutions, in relation to the strategic goals of the business has also been criticised for not delivering sufficient insights into the role of strategies and implementational plans. Hence, the design of information systems to detect threats or protect from attacks, will improve the management of cybersecurity when accompanied by the right strategies and implementational plans.

2.5.2.2.2 Security Risk Management

Risk management within the context of information-security risk has been recognised by many standards, frameworks, and best-practice guidelines. SSE CMM ,SEI, BSI and NIST have all indicated the importance of establishing an effective risk-management plan to improve the

organisational information-security resiliency (British Standards Institution (BSI), 2012; CMU, 2003; NIST, 2013; "SEI Capability Maturity Model's impact on Contractors", 1995). Establishing a holistic risk management that incorporates all risk functions has been increasingly challenging within FM organisations (Parn, 2019c). The digitalisation of processes accompanied by the adoption of BIM requires a holistic approach towards cyber-risks and physical-risks and their impact on the facilities as well as managing and maintaining stakeholders (Mayo and Snider, 2016). A holistic security-risk management entails the correlation of infrastructure, processes, procedures and people (Amin, 2019). It also includes the identification, analysis, mitigation and reporting of a cyber-risk and facilitates resiliency against its impact (Iden *et al.*, 2017). As proposed by many researchers including Mandani and Ramirez (2019), security-risk management is constructed upon the integration of IT security with business strategy. Hence, effective communication between the IT and business teams is required to achieve a holistic management of risk within a digitalised organisation, such as a BIM-FM organisation (Posthumus and Von Solms, 2004; Wood *et al.*, 2019).

2.5.2.2.3 Security Requirements Engineering

The engineering of the security requirements pertains to the identification of specific security-needs for the systems and infrastructure. This factor is acknowledged by many publications such as BSI (2002). As stated by Mellado *et al.*, (2010), the identification of systems-security requirements assists in achieving a robust plan for organisational cybersecurity-resiliency. This factor is accompanied by technological excellence, and is supported by continuous monitoring, improvement, and advancement. Acohido (2015) emphasises the importance of incorporating risk-management results within the engineering of security requirements, to ensure risk aware decision making in the development of identity-management plans, access control, incident-response plan, business-continuity plans, and configuration of information assets. Furthermore, the literature suggests the alignment of business teams knowledge of risk towards the business functions with the skill set and knowledge of both IT and technical security-specialists, to ensure an optimised design for the security requirements of systems (Glantz *et al.,* 2016)

2.5.2.2.4 Compliance with security regulations

As indicated by ISO 31000:2018, standardisation and compliance with the best practice guidelines and standards, positively contribute to the organisational cybersecurity-management approach (Hutchins, 2018). However, it has been identified that not many organisations within

the construction industry have adopted compliance to standards and best-practice guidelines (HM Goverment, 2015). Seeking certification from approved third party professional bodies who assess organisational strategies, processes and procedures against the best-practice security guidelines and standards, leads to an improved level of cybersecurity management (Mohan *et al.*, 2018). The literature also acknowledges the importance of an effective relationship between research, academia, professional bodies, and industrial organisations, to ensure an effective implementation of standards and regulatory guidelines (CERT, 2015).

2.5.2.2.5 Organisational modelling of information security requirements

Understanding and identifying the data-security requirements at an organisational level pertains to several factors. SEI, SSE CMM and ISACA have addressed the identification of the scale of risk tolerance as an important contributor to defining the organisational information-security requirements (CMU, 2003; ISACA, 2012a; "SEI Capability Maturity Model's impact on Contractors", 1995). To maintain a balanced approach towards securing information in the implementational tasks, strategic risk-aware decision making is required to take into account the risk-tolerance boundaries and business goals and objectives, and compare them against the threat impacts (Anderson and Choobineh, 2008; Ekstedt and Sommestad, 2009; Johansson *et al.*, 2006). The importance of recognising the level of information security required for the informational assets within an organisation has been indicated by (Liu *et al.*, 2012). However, this will have to be backed up by the realisation of the potential cost that may be incurred for an organisation to recover from a potential breach of cybersecurity (Edwards, 2018)

2.5.2.2.6 Defined security practices

NIST (2014, 2018), ISO/IEC 27000 and COBIT recommend that the implementation of cybersecurity strategies in organisations should rely on the transparent definition of their security practices. Bhattacherjee (2012) and Tsoutsos *et al.*, (2020) raised concerns regarding organisations whose primary operations were not focused on information security or providing technological solutions. Both studies demonstrated that developing formalised security practices is often forgotten. The Federation of European Risk Management Association (FERMA) and the British Standard ISO 31000:2009 also support the management of cybersecurity risks within organisations, using defined plans, processes, and procedures to identify, respond to, mitigate, or recover from, a malicious cyber-attack. Therefore, defined

cybersecurity practices are deemed as an essential determinant to successful management of cybersecurity within a digitalised BIM-FM organisation.

2.5.2.2.7 Continuous security process improvements

The nature of cybersecurity in the world today is ever changing (Nye, 2018). As stated in NIST, (2020), the evolution and advancements of technology has brought evolving cyber-threats to the digital systems and digitally-enabled organisations. Hence, the continuous improvement of security processes is emphasised, to enable organisations to keep up with the complexities of new threats and challenges. Across academia, many studies have pointed to the importance of change management within the strategies and processes (Fairholm and Card, 2009; Lacey, 2010). In this regard, Baskerville *et al. (*2002) insisted on the importance of accounting for the continuous change of strategy and process-redirection within an organisation, to enable an effective response towards the unpredictable needs of customers, stakeholders, systems and assets. Costello (2011) further recommends organisations to employ a rapid deployment of devices and systems, as well as a rapid upskilling in the use of new tools. Bechtold (1997) also pointed to the theory of continual change to the strategies, processes, and procedures, based on the feedback from various levels of an organisation. In support of the continuous process improvement, Leidner *et al.*, (2011) emphasised the vital need for such an approach in complex and dynamic organisations, such as FM, which entails the involvement and collaboration of many stakeholders on a wide range of projects. Hence, a continuous security process would empower the delivery of unique outputs with cybersecurity incorporated at every step of the process (Information security forum, 2005)

2.5.2.2.8 Competency of security team

The competency of the security team has been highlighted by Ekelhart *et al.*, (2009) and NIST, (2020), as a necessity when implementing and executing information-security strategies in an organisation. As stated by ISACA (2012) and Stanton *et al.*,(2004), the organisational management of information security relies upon the technical and institutional knowledge of the user, which determines the level of information-security maturity. Therefore, the cybersecurity knowledge of the technical teams and security specialists should be accompanied by knowledge of organisational strategies and working procedures (Kure *et al.*, 2018). Stanton et al., (2005) further elaborate on the alignment of the roles and capabilities of users for managing and maintaining the security of digital information. Hence, this determinant pertains

to the competency of the cybersecurity team in managing the security of information, taking into account the organisational goals and objectives (Kure *et al.*, 2018)

2.5.2.2.9 Security conscious employees

Bowen *et al.,* (2006) and NCSC, (2018) accentuate the inclusion of behavioural determinants in organisational cybersecurity-management models and highlight its importance in tackling insider cyber-threats and malicious activities by those trusted. (Smith and Brooks, 2013), found that improving cybersecurity consciousness in users resulted in an increase of 72% in their resiliency against phishing attacks. Cybersecurity awareness or consciousness has also been proposed by NIST, (2020), as a protective measure to support the ability of the organisation to minimise or evade the impacts of a potential cybersecurity attack (Liu *et al.,* 2009). The overriding importance of the cybersecurity consciousness of employees has been demonstrated by Griffin, (2019) and Kabanda, (2018), as an empowering support for the technical cybersecurity solutions. In improving the security consciousness of employees, Al-Janabi *et al.,* (2016) propose both effective communications to employees and organisational teams as well as continuous training, as a way of improving the cybersecurity culture of the organisation. According to Zwilling *et al.,* (2020), the cybersecurity consciousness of employees is the enabler of cybersecure decision-making within dynamic and complex organisations. Hence, embracing the challenges of a dynamic BIM-FM organisation is not possible without a combined technical and socio-technical approach to the management, that takes into account the behavioural aspects of employees as users (Malatji *et al.*, 2019).

2.5.2.2.10 Security leadership

Scovetta, (2013) has described leadership as the comparative analysis of the external factors, such as the market status, with internal factors, to set the right direction, vision, and mission for the organisation. Managerial behaviour and characteristics play an important role in the adoption of new technological advancements such as BIM within an organisation (Kuo and Lee, 2011; The International Organization for Standardization, 2012). Existing literature demonstrates that leadership and management qualities are the foundations of technology adoption, because of their empowering effect on the compatibility of both task and technology (Schumacher *et al.*, 2016). Bello, (2012) further elaborates on the performance improvements of employees that is achieved by leadership efforts, through working towards a shared goal. This concept is equally applicable to the cybersecurity-management initiatives and strategies that require prioritisation from the leadership, to provide effective intra-organisational

cybersecurity training and awareness programs (Joint Task Force, 2018). In leading the cybersecurity incentives of an organisation, it is the responsibility of senior management to align the cybersecurity strategy with business goals (Kayworth and Whitten, 2010). This would, in turn, encourage resource allocation towards cybersecurity-management processes and procedures (Amaio, 2009)

2.5.2.2.11 Business enablement of cybersecurity

Digital systems such as BIM are implemented to achieve increased profitability by reducing the need for financial and human resources and improving organisational competitive-advantage through operational efficiency (Smith, 2014). However, a cybersecurity strategy commonly requires additional resources, and does not always demonstrate an increased profitability in the short term (Hedström *et al.*, 2011). The process of managing and maintaining the cybersecurity of data is usually deemed as a labour intensive, time consuming and costly task that jeopardises financial goals (Scully, 2011). Hence, many industrial organisations consider cybersecurity reactively, after an incident takes place, at which point irremediable losses have incurred. These could include injury, loss of life, huge financial losses, and reputational loss (Scully, 2013). Therefore, it is important to assess the value of cybersecurity, by modelling the potential impact of a cyber-attack and understanding the implications following the compromise of a system (Lagazio *et al.*, 2014). This can in turn justify the requirements for implementing a cybersecurity strategy organisationally and will provide a clear understanding for the business teams (Borum *et al.*, 2015).

2.6 Primary Research Framework

Figure 6 illustrates the selected BIM-FM and organisational cybersecurity management determinants that contribute to an improved cybersecurity within a BIM-FM organisation.

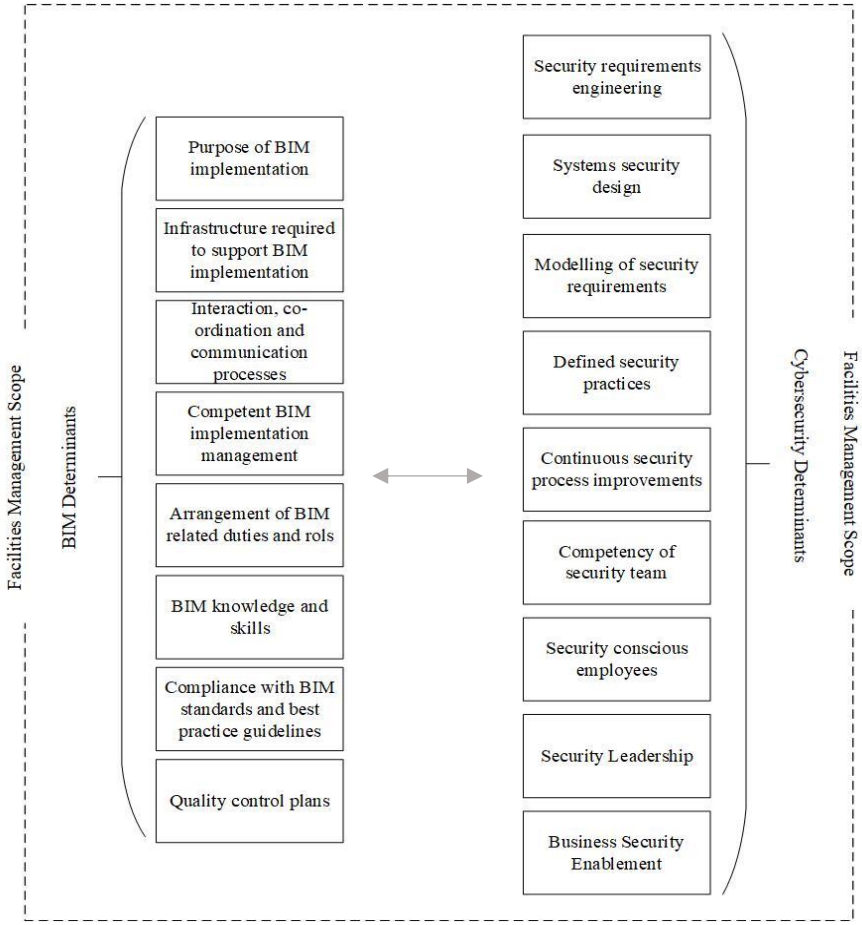


Figure 6- Synergy of Identified Determinants for a Cybersecure BIM-FM

Section 2.5 demonstrated limited literature on incorporating cyber security within BIM-FM. This is also accompanied by a lack of common guidance for implementing cybersecurity within BIM processes in FM, which has resulted an isolated approach towards cyber security management in BIM-FM organisations. Findings from the literature review further illustrate shortfalls and challenges within the strategic, implementational, and performance aspects of BIM-FM organisations in managing cybersecurity (section 2.3.3). Hence, the integration of cybersecurity determinants with BIM determinants, in strategy, implementation and performance layers of an organisation, would create a unified approach towards a cyber secure management of BIM-enabled facilities management organisations.

The strategic integration is directly associated with the organisational process of defining its strategy, direction and goals (Carter *et al.*, 1991; Casadesus-Masanell and Ricart, 2010; Martins and Terblanche, 2003). Decisions will be made for allocating resources in line

with the defined strategies and goals. Every strategy requires a robust action plan which encompasses the objectives and prepares for the implementation process (Kitchin and Kitchin, 2018; Oxtoby *et al.*, 2002; Peansupap and Walker, 2005). The integration of cybersecurity for BIM implementation is conducted through the identification of processes and procedures required (Khajuria *et al.*, 2017; Malatji *et al.*, 2020; McPhee and Khan, 2015) . The successful implementation of strategies is linked to the employee performance (Carter *et al.*, 1991; Supić, 2005). An organisation should efficiently execute its strategy to achieve its performance-improvement goals. The organisation culture is often the most important determiner for successful execution. Hence, performance management is often viewed from a perspective which considers both the culture and the people (Khorrami *et al.*, 2016; Kure *et al.*, 2018; Wamala, 2011).

Using the descriptions from sections 2.5.1.2 and 2.5.2.2, determinants were categorised under strategy, implementation, and performance. Thus, the primary research framework was structured as shown in figure 7:

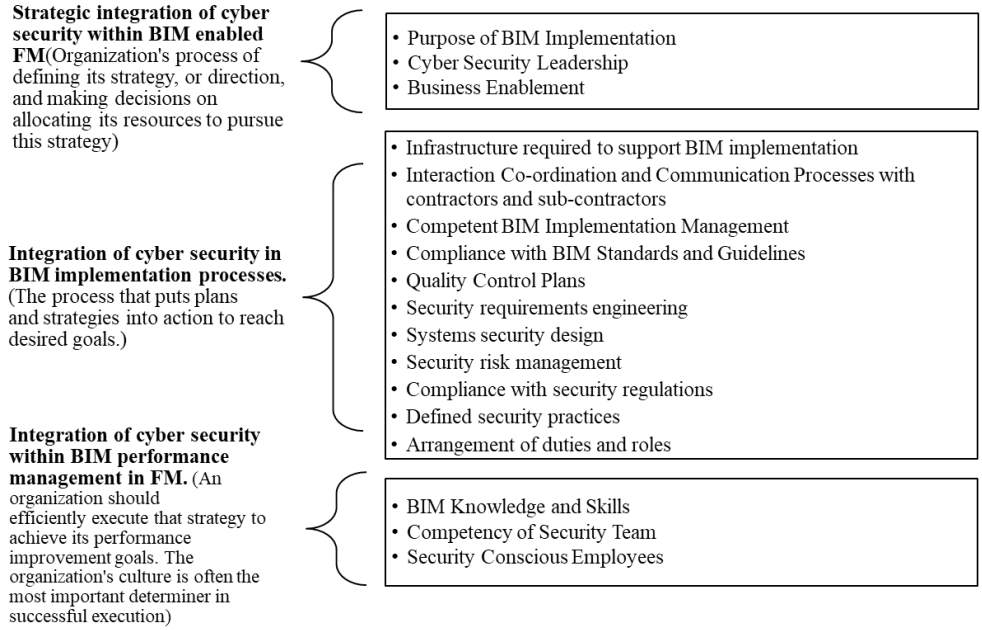


Figure 7- Primary Research Framework

2.7 Conclusion

This chapter offered a multi-disciplinary review of the literature in BIM, cybersecurity in the built environment and BIM-FM domains. The review of the literature in the BIM domain entailed the exploration of BIM project phases, data produced/exchanged at each stage and digital collaboration in BIM projects. The review of the literature in the cybersecurity of the

built-environment domain entailed looking at the concept of cybersecurity within organisations and in particular, organisations within the AECO industry. It demonstrated various cyber-threats, the potential impacts of cyber-attacks within the built environment, the cyber vulnerabilities introduced by digitalisation of the built environment, and the adoption of BIM within AECO organisations. The review of the literature identified the shortfalls and challenges associated with the issue of cybersecurity within the BIM-enabled AECO industry. Hence, a conceptual cybersecurity-risk model was developed to portray the cyber-risks associated with various phases of a BIM-enabled project. The model proposed that the criticality of cyber risk is relatively higher than in other phases of a BIM project, henceforth, the focus of the research was on the FM organisations. To further explore the issue of cybersecurity within BIM-FM, the implementation of BIM in various task areas of a facilities management organisation was reviewed. The benefits and challenges associated with the implementation of BIM was also identified.

Based on the findings in the cybersecurity domain, the impact of a cybersecurity breach in various task areas of a BIM-FM organisation was summarised in a BIM-FM specific cybersecurity risk matrix, demonstrating the criticality of risk and its implications on the facilities and their managing organisations. Therefore, section 2.5 identified the requirements that BIM-enabled facilities management organisations can seek to improve their cybersecurity profile. This was conducted by the secondary-data analysis to identify the determinants contributing to improved cybersecurity of BIM in FM. Through the exploration of maturity models, best-practice guidelines, standards, and peer reviewed journals, the social and managerial BIM determinants applicable to the FM organisations were extracted from the BIM-maturity models of both Succar and CIC. Also, the social and managerial determinants for organisational cybersecurity-management were extracted from the existing resources in the domain of cybersecurity management. The synergy of the extracted determinants formulated the primary-research framework. The following chapter outlines the approach adopted to validate and refine the framework.

Chapter Three: Methodology

3.1 Introduction

This chapter presents the research design and the methods used to answer the research question and achieve the research objectives. It provides a detailed explanation of the steps taken to respond to the research question and justifies the selection of research methodology and research design. It also discusses the underpinnings of designing research and the way in which it directs the researcher towards setting their priorities. In doing so, Section 3.2, discusses the philosophical positioning and world view of the researcher. This is followed by an overview of methodologies compatible with the philosophical positioning in section 3.3. Furthermore, Section 3.4 presents the research approach, which clarifies the reasoning behind the choices made. Section 3.5 provides a summary on the overall approach towards achieving the aim of this research project with reference to the existing literature on various philosophical concepts of the research design. This is followed by a discussion of the research methods in section 3.6, which describes the process of how knowledge is established in this research. Section 3.7 discusses the way the research quality is ensured, and section 3.8 concludes the chapter by identifying the ethical considerations that have been made throughout the study.

3.2 Research Philosophy

The theoretical perspective of a researcher represents the way in which they view the world and the reasoning behind every research assumption that is made throughout a research project (Gray, 2014; Saunders *et al.*, 2019). This theoretical perspective is known as the philosophical paradigm, or philosophical positioning, which supports the decisions taken in the research design and the choice of research methods for the purpose of achieving the research objectives (Leavy, 2017; Onwuegbuzie *et al.*, 2012). Saunders *et al.*, (2019) defines three main categories for the relationship between the process of creating knowledge and the output of that process, labelled as ontology (views of the world), epistemology (human knowledge of the world) and axiology (the effect of the researcher on the knowledge). Gray, (2014) states that ontology is concerned with the relative assumptions about the reality of knowledge. Ontological assumptions are characterised by two main categories, namely objectivism and subjectivism, which are stances at both ends of the ontological spectrum. Crotty, (1998) defines objectivism as a view where social objects are exterior to social actors, whilst subjectivism views social phenomenon as the result of the actions taken by social actors.

Saunders *et al.*, (2019) highlighted that researchers commonly implement an ontological view in between the two ends of the spectrum, depending on the research aims and objectives.

Considering the research aim (Chapter 1), identifying the requirements of a cybersecure management of BIM-enabled FM organisations from a socio-technical view requires an exploration of the interactions between people and technology, collaboration processes and the challenges involved in the handling and management of BIM project information. Therefore, a subjective ontological approach is required to acknowledge the subjectivity of the captured information about the reality, depending on the opinions and experiences of the social actors (e.g., BIM project stakeholders).

3.2.1 Critical Realism

A critical realist approach to the research supports the view that reality or truth exists regardless of human activities. However, it also appreciates that the complexities of the social world represent an open system that pushes access to the actual truth beyond reach (Carlsson, 2009). Critical realism acknowledges the assumptions regarding human knowledge, also known as epistemological assumptions, whilst being strongly focused on the ontological aspects (Sayer, 2000). As shown in figure 8, the critical realism view is based on the belief that the truth exists beyond our observations, however, our observations can increase our understanding of the unobservable structures that exist as part of the actual reality (Archer *et al.*, 2013; Mingers, 2004).

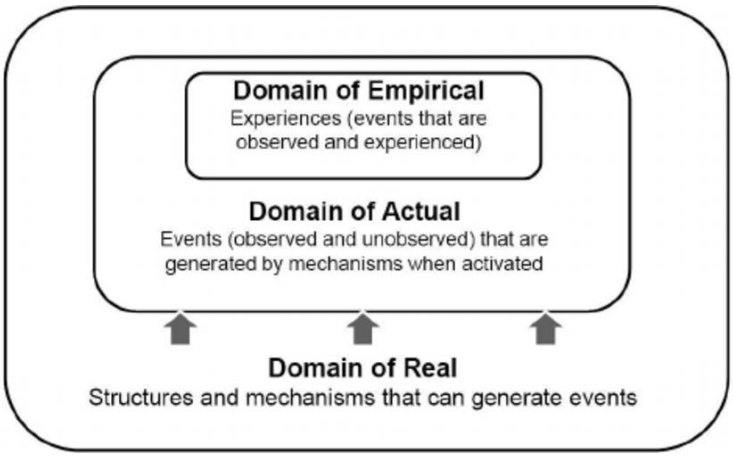


Figure 8-Critical Realism View (Mingers, 2004)

Although an interpretivist philosophical stance holds similar views to critical realism, it overlooks the unobservable of the truth by solely depending on understanding the phenomenon from the perceptions and experiences of the individual (Capps, 2019). Alternative

philosophical stances such as positivism would be suitable for research where an existing theory is subjected to test and evaluation (Myers *et al.*, 2004).

Thus, approaching this research from a critical realism perspective, acknowledges the subjectivity of the knowledge that is captured about the actual reality (Saunders *et al.*, 2019). Therefore, the axiological considerations, pertaining to the effects of researcher on the creation of knowledge should be discussed. Hence, the collection of empirical and theoretical knowledge and their synchronisation would assist the researcher with better interpretation and apprehension of knowledge. Furthermore, the self-awareness of the researcher regarding the possible biases raised by the beliefs, gender, background, and other positions of the researcher are also important in collecting and interpreting information throughout the process of research. Thus, in the process of data collection and analysis of this study, to avoid bias, the researcher sought neutrality in the approach taken.

3.3 Methodology in Critical Realism

Yin, (2014) define research methodology as the underpinning principles, processes, and procedures of a scientific investigation. Saunders *et al.*, (2019) state that the logical thought process and philosophy of reasoning supports the application of a research methodology and the choice of research methods. As discussed in section 3.2, this research is based on a critical realism philosophy of reasoning. Although critical realism is compatible with both qualitative and quantitative research methods (Zachariadis *et al.*, 2013), it has also been postulated that qualitative methods are more aligned with critical realist views (Mingers *et al.*, 2013). This is due to the capability of qualitative methods for exploring meaning through the perspectives, experiences, and thoughts of the participant, and therefore, enabling a better understanding of the stance of the researcher, in relation to the reality (Yin, 2018). In contrast, quantitative methods fall short of providing an in-depth description of the matter under investigation, and have limited capability for explaining the interactions between complex mechanisms. (Mingers *et al.*, 2013) and Sayer (2000),also acknowledge that although critical realism allows flexibility in the choice of research methods, the nature of the matter under investigation and the aim of the study should also be considered. As this research aims to incorporate cybersecurity considerations in BIM-FM, in-depth understanding of the concepts of BIM, cybersecurity, and the interaction and experiences of people with technology is required. Therefore, this research mainly uses qualitative methods to enable in-depth exploration of the concepts under investigation.

3.4 Research Approach

Creswell, (2015) suggested that the research approach is the way in which the researcher plans the roadmap towards the collection and analysis of data. There are various research approaches, including inductive, deductive and abductive (i.e. a combination of inductive and deductive), which are used to tackle research of different nature and scope (Pohontsch, 2019; Woiceshyn and Daellenbach, 2018). A deductive approach commonly begins with a theory which might be subjected to further expansion or modifications, and then later tested and evaluated. This approach is usually accompanied with objectivism and is popular in the natural sciences and for the clarification of concepts and phenomenon (Bradford, 2017). A deductive research approach involves the collection of data to assess a hypothesis, with the aim of approving or rejecting the underpinning theory (McGhee *et al.*, 2007; Pohontsch, 2019).

Alternatively, as shown in figure 9, an inductive approach is commonly accompanied by subjectivism, where the process commences with exploratory observations (Trochim and Donnelly, 2001). In light of this, Bryman, (2016) adds that an inductive approach involves exploration and observation of the phenomenon, leading to the formation of hypotheses that are later explored to provide general conclusions.

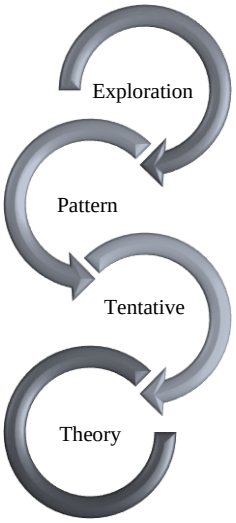


Figure 9-Inductive Research Process (Trochim and Donnelly, 2001)

Kothari, (2004) and Merriam, (2009) also assert that the inductive approach to research involves open-ended exploration during the preliminary stages of the project, that facilitates the apprehension of meanings and their social connections to events. In contrast to the deductive approach, inductive research is usually associated with the collection of qualitative data, where the flexibility of the research design allows for the change of research focus throughout the process (Oleskeviciene *et al.*, 2020). Whilst a deductive approach is concerned

with large sample sizes to generalise the findings, an inductive approach is more concerned with constructing a knowledge block that facilitates an in-depth understanding of the research topic.

Considering that the research aims to incorporate cybersecurity considerations in BIM-FM organisations, preliminary exploration of the subject was required to identify where the issue lies. Therefore, an inductive approach was suitable to be employed to allow open-ended exploration of the topic in multiple domains of BIM and cybersecurity in the built environment. Given that cybersecurity entails the interaction of people with technology such as BIM, an inductive approach also enabled the investigation of the social aspects, where the subjectivity of knowledge is taken into account (Kothari, 2004; Oleskeviciene, 2020). Thus, this research commenced with a review to identify the gaps in the literature for BIM and cybersecurity in the built environment, which directs the focus of the research to the socio-technical aspects of cybersecurity in BIM-FM organisations.

3.5 Research design

Research design is a sequential representation of the way various components of research such as aims, objectives, research methods, techniques and boundaries connect (Creswell, 2015). (Bryman, 2016) state that the research design demonstrates the application of research methods and data analysis in the research. Yin, (2014) also states that the research design portrays the ways in which the application of the selected research methods and data analysis techniques lead to the development of responses to the research questions. Creswell and Poth, (2016)further point out the connections between the research methodology and the philosophical positioning (paradigm) of the research and emphasise the importance of research design in elucidating the research process. Hence, in a research design, the nature of the problem under investigation, philosophical positioning, timeframe of the research, and resource availability must be taken into account to prevent any potential shortfalls (Saunders *et al.*, 2019; Yin, 2014). This will ensure the repeatability of the research by acting as a map that represents the interconnections of the steps taken along the research process (Maxwell, 2013). Royer and Zarlowski, (2001) state that research design is part of the research process and is formed following the identification of the research theme. It entails exploratory research into the research theme and leads to the formation of research questions.

The preliminary literature review of cybersecurity and BIM illustrated that the issue of cybersecurity is critical within the in-use phase of the BIM lifecycle, therefore, the focus of the

research was directed to the BIM-FM organisations, as the main stakeholders involved in managing and maintaining the facility in the in-use phase. It showed that the cybersecurity vulnerabilities within organisations are overly dependent on the technical cybersecurity solutions provided by infrastructure suppliers and IT teams to manage the cybersecurity of information. Therefore, the focus of the research was further narrowed down to the people and process aspects of managing cybersecurity in BIM-FM organisations. Hence, the research question and the succeeding research objectives were developed (chapter 1).

To fulfil the second research objective, a critical review of the literature was conducted to highlight the challenges associated with the implementation of BIM in FM, that heighten the risk of a cybersecurity attack in BIM-enabled facilities management organisations. The literature review was further expanded to explore the complexities in the management of cybersecurity BIM-FM, whilst highlighting the people and process aspects of cybersecurity in BIM-FM.

In fulfilling the third research objective, the requirements of a cybersecure BIM-FM organisation were investigated. This entailed the collection of theoretical data from secondary information sources and empirical data from semi-structured interviews with industry professionals. The collection of data from two different sources improves the quality of the results and assists the researcher in the interpretation of information. Owen, (2014) and Taylor, (2012) assert that the assimilation of various qualitative methods, such as qualitative exploration and analysis of secondary data, followed by semi-structured interviews, results in justifiable research findings. Therefore, the next stage of the research was designed to analyse the information collected through the second stage.

Dixon-Woods *et al.*, (2005) suggest that thematic analysis explores the similarities, diversity, typologies, and existing trends in the existing resources and hence offers an in-depth insight into the interconnections between various themes. Thematic analysis of both primary and secondary data led to the next stage of the research, where the research framework was developed.

Finally, following the synchronisation of all findings, a qualitative validation of the research framework was conducted through experts' review. Sandelowski (1998) suggests that in validating qualitative research, experts can best criticise the research outcome by asking the right questions, not by providing the right answers. Sandelowski, (1998) further elaborates on

this by saying that experts can assist the researcher in resolving the shortcomings and defects of the final research product.

The research design, as presented in Figure 10 below, was thus constructed to plan the process of fulfilling the research objectives.

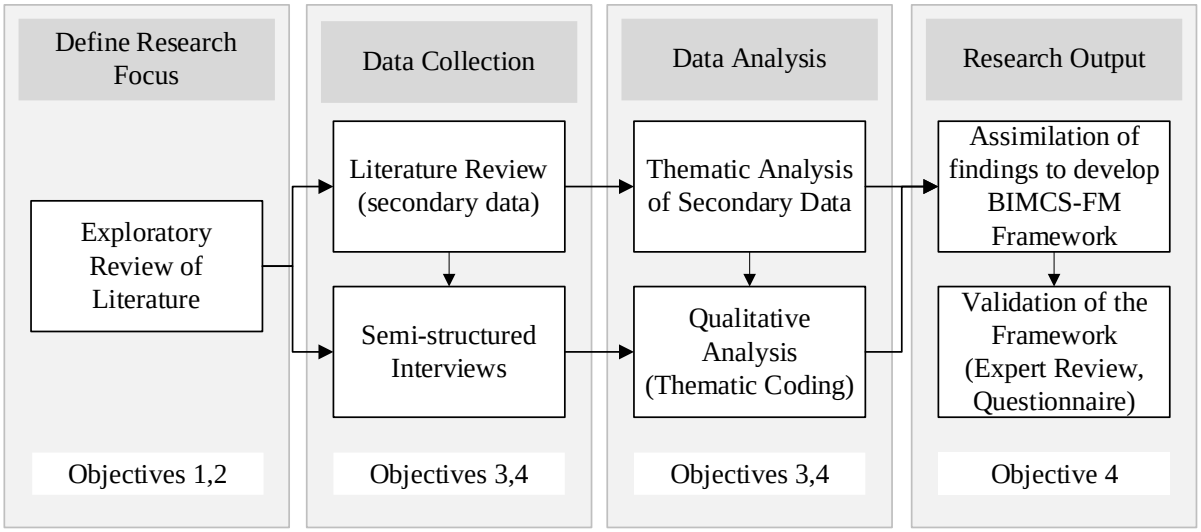


Figure 10- Research Design

3.6 Qualitative Research Methods

Qualitative research methods transform reality into various representations, such as a discussion, interview, photograph or memo (Denzin and Lincoln, 2000). In this research, to identify what makes a cybersecure BIM-enabled facilities management, in-depth knowledge of collaboration processes and procedures, and an understanding of the way BIM-FM organisations manage and handle digital information is required. FM professionals' experience and perspective provide meaningful insights into the challenges of a cybersecure implementation of BIM in FM. Cresswell (2018) points out the importance of the viewpoints of participants and the subjectivity of their perspectives, which are captured during the course of a qualitative data collection. Therefore, this research used interviews to capture the understanding and insights of FM professionals regarding the concepts of BIM and cybersecurity.

A key characteristic of qualitative research methods is the effect of researchers on the collection and analysis of data (Cresswell, 2018). To minimise the researcher-bias it is recommended to use multiple sources of data such as documents and images is recommended to enable comparison and improve the accuracy of the results (Merriam, 2009). Thus, this research collects theoretical data through the review of literature, to allow more accurate interpretation

of empirical results. The synchronisation of both empirical and theoretical findings then forms the research output.

The choice of research methods used in the collection and analysis of data is explained in the following sections:

3.6.1 Preliminary Explorations- Review of Literature

The first stage in the design of this research entailed a broad exploration of both BIM and cybersecurity domains (research objective 1).This was carried out through a literature review, with the aim of establishing knowledge and apprehension of the current research in both domains. Snyder (2019) stated that a literature review describes the stance of existing studies and their contribution to the understanding of the research problem under investigation. Snyder (2019) further suggests that a literature review enables new interpretations of the previous studies and leads to the identification of the areas in need of additional work. Steward, (2004) further emphasise that the review of literature illustrates where the research focus lies in the context of the existing studies. The review of the literature for BIM and cybersecurity in the built environment domain demonstrated that the impact of cybersecurity risks is critical within FM organisations. Thus, the research focus was narrowed down to the cybersecurity of BIM-enabled facilities management organisations, which encouraged further investigation of the literature (research objective 2) in the application of BIM in FM, to fulfil the second research objective.

The review of literature illustrated the cybersecurity risk and vulnerabilities in BIM-FM organisations. Further investigation also demonstrated that BIM and cybersecurity concepts were commonly coupled from a technical point of view, which impedes the people and process aspects of cybersecurity of BIM-FM. This resulted in a further demarcation of the research focus to the people and process aspects of cybersecurity management in BIM-FM (research objective 3). Therefore, the third research objective was approached from a people and process perspective.

3.6.2 Secondary Data Analysis

Hakim (1982) defined secondary data analysis as “any further analysis of an existing dataset which presents interpretations, conclusions or knowledge additional to, or different from, those presented in the first report on the inquiry as a whole and its main results”. Secondary data analysis is particularly used in multi-disciplinary studies where a primary approach to data

collection often requires high levels of expertise in all targeted disciplines that may not be present within a small group of researchers (Cheng and Phillips, 2014). Although using secondary data means a larger breadth of information can be used from various resources, they may not always include the response to the questions of the researcher (Boslaugh, 2009). In topics of a multi-disciplinary nature, the existing resources may only address one area of the research focus, therefore, an assimilation of resources might be required to cover all aspects of the research (Gale *et al.*, 2013).

The third research objective seeks to identify the people and process related determinants of a cybersecure BIM-enabled facilities management (see secondary data analysis in figure 11). This entailed looking at multiple disciplines of cybersecurity and BIM-FM from both social and managerial perspectives. Although various BIM maturity models have previously identified the determinants of a successful implementation of BIM, limited consideration has been given to the people and process aspects of cybersecurity. Therefore, best practice guidelines and standards, as well as peer-reviewed journals in cybersecurity management were used to identify the people and process related cybersecurity determinants, applicable in BIM-FM organisations (figure 11).

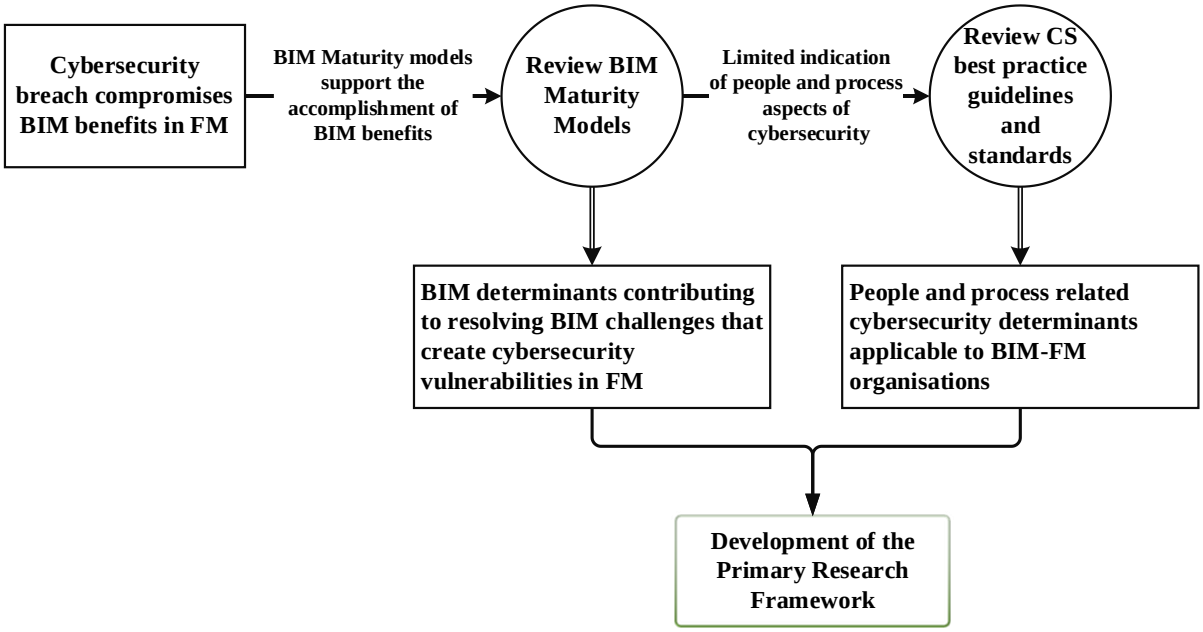


Figure 11- Multi-disciplinary analysis of secondary data for identification of determinants

The extraction of determinants from various resources was achieved using the thematic analysis of secondary data. This is concerned with identifying the knowledge and core elements together with an evaluation and coalition of the existing resources to depict specific aspects of

the phenomenon (Braun and Clarke, 2012). Thematic analysis was chosen because the problem required knowledge from multiple disciplines regarding both cybersecurity in the built environment and BIM-FM. As per Dixon-Woods *et al.*, (2005), thematic analysis explored the similarities, diversity, typologies, and existing trends in the existing resources and hence offers an in-depth insight into the interconnections between various themes. The selected resources were explored, and findings were interpreted by the researcher, to enable appreciation of the interchangeable phrases and terminologies used to communicate the meanings and concepts of the phenomenon. The resources were manually selected based on the scope of the research, filtered by inclusion and exclusion criteria, and bounded by the key focus of the publication. Following the review and analysis of this first set of publications, a subset of these were considered for further review with respect to their relevance, focus and research domain selecting only those with a social and managerial focus to BIM and cybersecurity, whilst omitting those concentrating purely on the technical aspects.

Through the assimilation of findings identified from the cybersecurity and BIM data sources, the primary research framework was proposed which integrated both cybersecurity and BIM-FM determinants. The concepts proposed by the framework required further investigation, to ensure they were fit to fulfil the third and fourth research objectives. Hence, the next stage of the research involved collecting primary data, to expand and revise the primary framework.

3.6.3 Primary data collection- Interviews

Eriksson and Kovalainen, (2008) suggested that interviews enable the researcher to gain an insight into both real-life experiences and expert opinions regarding the matter under investigation. Furthermore, interview is a common research method within qualitative studies that elicit various perspectives in the form of discussions between the participants and the researcher (Qu and Dumay, 2011). Structured interviews are those designed with a previously constructed set of questions. As per Stuckey, (2013), this type of interview allows for the speedy collection of data with the lowest potential for bias. However, Lewis-Beck *et al.*, (2012) have criticised this method as being susceptible to bias, because the demarcation of conversation through structured questions might induce specific point of views or omit opinions that fall outside the boundaries set by the researcher. An alternative option is the unstructured interview, where there is a high level of flexibility in the discussions between the participant and the researcher (Qu and Dumay, 2011). However, it does not allow further exploration of the concepts already extracted from the secondary data collection. The

discussions should address the objectives, whilst allowing the collection of new knowledge. Unstructured interviews have the risk of not hitting the targeted research domain, as the participants are responsible for choosing what is relevant (Woods, 2011).

The semi-structured interview was chosen because it has the advantage of having a structure within the boundaries of the research objectives whilst allowing for further knowledge to be shared (Adams, 2015). Semi-structured interviews allow a degree of flexibility in the discussions, whilst ensuring the conversation is not heading in the wrong direction. (Myers *et al.*, 2004) states that in a semi-structured interview the questions allow the respondents to share their opinions openly, however, the discussions can be kept within the boundaries, by using prompting and probing questions. Sapsford and Jupp, (2012) further suggest that semi-structured interviews also allow the researcher to repeat a question or slightly change the wordings and phrases to achieve more precise responses from the participants. Also, Bryman, (2016) states that a semi-structured plan of an interview is deemed as an interview guide, that maintains the balance between flexibility and the research boundaries. Therefore, using semi-structured interviews in this research enables further expansion and exploration of the determinants proposed within the primary research framework.

3.6.3.1 Interview Set-up

The undertaking of interviews can be done through various settings, including face-to-face (in-person) interviews, telephone/audio calls or videocalls (Stuckey, 2013). Each setting is associated with a number of advantages and disadvantages. The advantages associated with an in-person interview is the non-verbal communication and the facial expressions that are observed by the researcher during the interview session. These can assist the researcher to clarify any doubts and confusions instantly (Woods, 2011). However, this set up requires a higher level of communication and improvisation skills. More importantly, meeting in person with all the participants is time consuming, difficult to arrange and is commonly associated with geographical barriers (Sekaran and Bougie, 2016). Although the interviews in this research were primarily planned to be undertaken in a face-to-face setting, a global pandemic resulting in a nationwide lock-down of all businesses and institutes arose during this phase of the research project, hence, the researcher considered audio calls as an alternative setting for conducting the interviews. This choice also had a number of advantages including overcoming geographical limitations. Audio calls were significantly more convenient for most participants and certainly helped with interviewing a larger sample. It was also advantageous in cases where

respondents felt pressure and a degree of anxiety to attend an in-person interview session (Flick *et al.*, 2015; Kvale, 2011a). Despite the advantages, some disadvantages regarding technological challenges (i.e. a low signal/internet connection) as well as missing out on the non-verbal expressions were identified as the limitations of this set-up (Allmark *et al.*, 2009; Knox and Burkard, 2009). Although the latter disadvantage could be partly resolved using video calls, a number of participants expressed that they would prefer an audio call due to them needing to work from home and also having weak internet connections that did not allow for a video call without interruptions. Hence, to maintain consistency, audio calls were used to collect the empirical data.

3.6.3.2 Structuring interview questions

Findings from the literature review were used as a guide for structuring the interview questions. Questions were designed to address strategic, implementational and performance-related aspects of cybersecurity integration in BIM-FM. Although the questions were set to further address the identified determinants from the secondary data analysis (i.e., the lead determinants), they were flexible to allow any new knowledge to be discovered through the exploration of the experiences of professionals in practice. The empirical data also allowed an overview of the existing trends in practice, and hence, enabled comparison with the findings of the secondary data analysis through interactions with industry professionals. The focus of each interview question is discussed in section 4.2.2.

3.6.3.3 Participant Selection

Findings illustrated that the cybersecurity vulnerabilities arise from the challenges associated with the mature implementation of BIM in FM. Therefore, the interviews aimed to collect the perspectives, understanding and experience of FM in managing the cybersecurity of data in BIM-FM organisations. For this purpose, FM professionals with knowledge and experience of working in a BIM-FM organisation would provide the required information. The selection of this sample can be rationalised by the complex phenomenon investigated in this research which requires the contextualising and in-depth understanding of FM, but more importantly BIM-FM. Hence, the experts targeted would support identifying issues related to cybersecurity within BIM-enabled FM. As the primary research framework propose determinants within the strategy, implementation and performance layers of an organisation, individuals in senior positions and key decision makers within BIM-enabled FM organisations were targeted to

capture their experience and insights on the issue of cybersecurity management. The roles of the participants and the sector of their organisations are tabulated in table 4.

Table 4- Participants' Roles & Organisational Sector

Interviewees' roles	No.	Organisational Sector (No. of Participants)
Project Manager	3	General Contractor (2) Commercial/Residential (1)
Facilities Management Director	4	General Contractor (3) Education (1)
Facilities Manager	5	Commercial (2) Health (1) Residential (2)
Head of Information Management in FM	2	General Contractor (2)
Head of Technology & Innovation in FM	1	Public/Commercial (1)
Managing Director of FM	2	Commercial/Residential (2)
Director of Estates & Facilities	1	Education (1)
Associate Director of Technology in FM	2	Financial/Commercial
Head of Digital Transformation in FM	1	Education (1)

BIM-enabled facilities management is still at its early stages of transition and hence, finding professionals with experience of working in BIM-enabled facilities management organisations required a multi-step approach to finding the ideal participants that would meet the selection criteria for the data collection. Participants for the interviews, were selected based on their expertise in BIM-FM.A direct approach being made to professionals within the facilities management organisations who have adopted BIM as their modus operandi or have been involved in BIM-enabled projects. Almost all participants were initially either contacted via professional social-media platforms such as LinkedIn, or their professional email address. Furthermore, the experiences of participants were examined with specific focus on management positions (e.g., facility manager, project manager, information manager, innovation manager). Following the primary contact with the selected participants, some snowball referrals took place with peer recommendations.

As Saunders et al., (2012) state, the sample population (also labelled as the sampling frame) is representative of the whole total. Various methods are utilised to distinguish the representative sample from the grand total, including systematic sampling, simple random sampling, non-probability and many more. In the context of this research, determining the total population would be unfeasible, considering the various states of BIM maturity in FM, and the variety of BIM use in organisations (ad-hoc, organisational implementation, etc).Also, the interviews were not aimed at reaching a saturation point, but to achieve an in-depth understanding of the

issue. Therefore, 25 professionals in senior positions with relevant knowledge and experience of working in a BIM-enabled FM organisation were selected to be interviewed. With the chosen interview setup being audio/phone calls, the participant selection was not limited to geographical restrictions, hence, adding to the value of the primary-data collection (Kvale, 2011a)Considering that the BIM regulations and working processes differ around the world, only organisations operating within the UK were considered for participant selection. Furthermore, due to the differing characteristics of various industries, in terms of the available resources, government support, and nature of work, the participants were selected from facilities management organisations from a variety of industrial sectors (e.g., education, healthcare, etc). The decision to employ purposive sampling supports the achievement of new insights into the matter under exploration (Saunders *et al.*, 2019). The research specified that the selection of participants should be based on their knowledge and experience of BIM projects and their history of working with, or within, a facilities management organisation. Therefore, participants were selected from various organisations with various roles (e.g., Facilities Manager, Information Controller, Project Manager, etc.) to ensure that a balanced representation of strategic and operational roles were represented within the data. The participants selection was undertaken regardless of gender to avoid any bias.

3.6.4 Thematic Analysis of Data

The number of qualitative studies using interviews as their method of data collection has grown over the last couple of decades, and there are many studies of how to undertake interviews. However, studies describing the process of developing, analysing and validating qualitative interviews are still exceedingly rare (Kvale, 2011a). As per the approach to qualitative data analysis proposed by O'Leary, (2021), a valid analysis of interviews can be achieved by following five key steps, as used in this research, which were:

i. Review and revise interview transcripts to understand the content and for the identification of certain patterns, themes, or new ideas.
ii. Develop descriptive and interpretive categories using the contents of the transcripts and the preliminary review of the literature.
iii. Revise the content within each category, to determine any existing inter-connections.
iv. Develop a set of codes that best represents the knowledge and meaning within the transcripts.

v. Revise the primary set of codes, to narrow down the code list and identify the themes that best contribute to the research question.

For the transcription of the interviews, the researcher opted for a verbatim transcription of the interview sessions, rather than limiting the data to the selective transcription of the interview discussions. As per Kvale, (2011a) this ensures that no information is overlooked during the analysis. Following a thorough review of all transcripts, the researcher chose to input the transcripts into NVIVO12, which is a qualitative data analysis software tool that enables the structuring, analysis, and representation of qualitative data. The decision to use this software tool was made, based on its ability to store, structure and analyse large volumes of qualitative data (Tookey *et al.*, 2011).

3.6.5 Framework Validation: Expert's Review

Validation of the research output requires the examination of a body of evidence from other research, both causal and descriptive, drawn from other experiences or settings, or from reflective practitioners (Leviton, 2015). This research used expert's review to validate the research output (i.e., the BIMCS-FM framework). Expert review or judgement is a common method used for validating a framework's relevance, applicability, and representativeness for a particular phenomenon (Haynes *et al.*, 1995). As defined by Escobar-Pérez and Cuervo-Martínez (2008), this method provides informed opinion, judgement, and assessment from qualified experts with a track record of experience/knowledge on the research topic. The comments collected from the experts are used to add or omit elements, or to improve the clarity of the concepts proposed by the research construct (Garrote *et al.*, 2015). In conducting validation using expert opinion, identifying the expert selection criteria as well as the method of data collection play a key role. The selection of the experts is often based on their theoretical or practical knowledge of the topic under investigation, however, alternative criteria can be considered, depending on the purpose of validation and research characteristics (Escobar-Pérez *et al.*, 2008). Various methods can be used to collect experts' opinion, either individually or in groups. These methods can result in either qualitative or quantitative judgement of the strength and weaknesses of the research construct (Hyrkäs *et al.*, 2003). In using expert review as a way of validating the research construct, correct performance of the procedures is of great importance. Therefore, employing formal methods in the selection of the experts, and the collection and analysis of data, will improve on the soundness of the results (Escobar-Pérez *et al.*, 2008)

3.6.5.1 Expert selection criteria

Beecham *et al.*, (2005) suggests that tactical experts with experience and knowledge of the subject matter improve the scientific validity of the study. Therefore, the selection of experts was based on their knowledge and experience of either BIM-enabled facilities management or cybersecurity management in organisations. The purpose was to validate the research framework using experts from both backgrounds to ensure the aspects of both cybersecurity and BIM-FM were considered. Only experts in senior management positions were selected, to incorporate their experience of management and implementation in their feedback. Therefore, the validation of the framework was conducted using seven experts, to allow the collection of their perspectives and opinions. The roles and organisational sector of the respondents are shown in table 5 .The steps taken to select and contact the experts is detailed in section 6.2.

Table 5- Participant's Roles & Organisational Sector

Participants' roles	**No.**	**Organisational Sector**
Head of Digital Asset Security in FM	1	Public
Cybersecurity Consultant for FM	1	Construction/Engineering/FM
Facilities Manager	2	General Contractor
Information Manager in FM	2	Public/Commercial
Project Manager in FM	1	Education

3.6.5.2 Open-ended questionnaire

In selection of the data collection method, qualitative methods were considered to enable a richer insight into the opinions and thoughts of the experts. The choice of an open-ended questionnaire over other methods, such as interviews or focus groups, was made by considering the purpose of validation, the characteristics of the research output and the sensitive nature of the topic under investigation. The BIMCS-FM framework developed following the assimilation of both the theoretical and empirical findings of this research, encompass a number of determinants and their interconnections within the three layers of strategy, implementation, and performance. The description of each of the determinants together with an introduction to the framework and its purpose was also developed to give the experts a better understanding of the research output. Considering the complexity of the framework, a questionnaire enabled the experts to spend time reading and comprehending the definitions and framework description and provided a more comprehensive response to the validation questions. This would not have been accommodated within a focus group or interview setting, where a spontaneous response and engagement in the discussions is required of the experts. Also, the

open-ended design of the questionnaire enables the experts to freely express their opinions and allows suggestions for new additions to the framework. Alternative methods such as focus groups would also enable rich discussions and extraction of new ideas, however, being focused on organisational cybersecurity management, the sensitive nature of the framework would limit the expression of ideas in a focus group setting. Hence, the experts were provided with an open-ended questionnaire (see section 6.3 and 6.4), and sent to the experts, together with the description of the framework and the description of the proposed determinants. Upon the return of the questionnaire, the feedback of the experts was qualitatively analysed to assess how the responses addressed the purposes of the validation.

Although the use of a questionnaire for expert validation is well established, it is recommended that the validation of any research construct using this method should be continually reviewed and improved. Therefore, the research quality is also addressed in section 3.7, which explains the reliability of the methods and techniques used during the research process.

3.7 Research Quality

Empirical data in qualitative research has often faced criticism and scepticism as to whether the research presents reliable results (Pohontsch, 2019). In this regard, Allmark *et al.*, (2009) emphasised the importance of maintaining high quality throughout the research design and analysis. The research quality represents the reliability and trustworthiness of all aspects of research. As stated by Leavy, (2017), research reliability is an indicator of the quality of the methods and techniques used within qualitative research.

Despite the emerging number of qualitative studies, a limited number of resources have described the validation processes for the quality of qualitative research, particularly for those involving in-depth interviews. Research quality is often addressed by reference to explicit criteria that leads to a transparent research methodology that can accurately report on the strength and limitations, whilst optimising the quality of research throughout (Eriksson and Kovalainen, 2008). It has been argued that in order to establish the research quality, the research paradigm, types of data and data analysis procedure should be taken into consideration and accurately incorporated within the research methodology (Bryman *et al.*, 2008). Hence, the following section will describe how the research quality was maintained throughout the research process.

3.7.1 Reliability and Trustworthiness

Research quality represents the reliability of the methods and techniques used to achieve the objectives of the study. This also involves the trustworthiness of the research in all aspects, including all processes and procedures to collect, analyse and report data (Pohontsch, 2019). In the context of this research, consistency, transparency, and accuracy were sought in reporting the research design, methodology and findings, based on high moral principles (Beecham *et al.*, 2005). For instance, to ensure a transparent and consistent approach to primary data collection, interviews were audio-recorded and followed by verbatim transcription techniques (Cohen and Crabtree, 2006).

In qualitative research, using semi-structured interviews, where a degree of flexibility is required to explore deeper aspects of a phenomenon, replicability is a challenge (Lewis-Beck *et al.*, 2012). Considering the variations in the personal attributes of the researcher, such as interview skills and research skills, a degree of variation is inevitable (Sapsford *et al.*, 2012). Hence, the possibility of achieving the same results with the same techniques by another researcher might be affected (Bryman *et al.*, 2008). However, bias as such can be minimised by first acknowledging that each researcher has their own way of explaining concepts, and secondly, seeking to use a standardised procedures (Noble and Smith, 2015). For instance, in this research, efforts have been made to ensure interviews were conducted in accordance with the interview guide (i.e., by semi-structured questions), with minimum variations and with specific focus on the lead determinants, derived from the secondary data analysis. Furthermore, the researcher sought to document every step of the data collection and analysis with maximum possible transparency and precision. Thus, the aforementioned steps inherently improve on the credibility of research and increase the reliability and trustworthiness (Bhattacherjee, 2012; Lewis-Beck *et al.*, 2012; Sapsford *et al.*, 2012)

An alternative criterion representing the trustworthiness of the research, is the research rigour, which is described as the quality of findings, or the contribution that results from the output of the research (Bryman, 2016). This particularly represents the authenticity of the interpretations of researchers regarding academic standards, based on various forms of internal and external validity (Myers, 2013). In the light of this, Flick (2008) states that qualitative research validity is strongly dependent on the trustworthiness of the data collection and analysis and the reporting of the findings. Hence, in the context of this research, the rigour is assured through

the transparency, trustworthiness and reliability of the processes, procedures, and methods used (Bashir et al., 2008).

3.8 Ethical considerations

This research was conducted in compliance with the Birmingham City University research ethics rules and regulations. Substantive percentages of this research have relied on secondary data, including the literature review that entailed the use of peer-reviewed journal papers, best practice guidelines and standards, maturity models and frameworks. Hence, note taking and precise citation of the resources was implemented throughout the research (Bloomberg and Volpe, 2018). The primary data collection through interviews with 25 participants, was performed based on the ethical practices of Birmingham City University and the appointed supervisory team. In the pre-interview phase, all respondents were provided with a research-participants brief which included a summary of the research, the purpose of data collection and how they will be contributing to the creation of knowledge for this research. Furthermore, the document elucidated the confidentiality and anonymity of the information given by participants. In the light of this, the participants were asked for permission to use their responses in the research and were informed of their right to withdraw from the research at any given time. Hence, the involvement of participants in the data collection was fully voluntary, with comprehensive information about the procedures of the interviews, recording of the interview sessions and their rights specified to them (Rudestam et al., 2014). As recommended by UK Research and Innovation (UKRI), a formally written consent form signed by all participants, affirmed their understanding and appreciation of their ethical rights, the potential risks and benefits to them, the research processes and procedures used, the level of their involvement and any other relevant information. Hence, every effort was made to articulate and communicate the aforementioned information to all participants, prior to the data collection.

The ethical considerations should also be addressed in the design of the interviews (Kvale, 2011b). Hence, in the design of the interview questions within this research, effort was made to ensure questions were not distressing to the participants, by omitting any psychological, personal and/or brand specific questions that might disregard the confidentiality, anonymity, and professionalism of the interviews. Sections 3.9.1 and 3.9.2 illustrate the way in which anonymity and sensitivity of the interview questions were managed and controlled in favour of the participants and in accordance with the ethical rules of the BCU research regulations.

3.8.1 Confidentiality & Anonymity

To ensure all the ethical considered were addressed, the researcher was responsible for managing and maintaining the confidentiality of the personally-identifiable information, that might pose risks and create undesirable consequences for the participants and their organisations (Allmark *et al.*, 2009). Many studies have accentuated the importance of codifying personal information to preserve the rights of the participants and avoid any negative implications for those involved (Rudestam and Newton, 2014). The terms "confidentiality" and "anonymity" are commonly used jointly. Confidentiality is the secure management of information to ensure that the information is not used for any purpose other than that stated and is secured from unauthorised access (Wiles *et al.*, 2008). Harding, (2018) stated that anonymity is obscuring the source of identity, and hence, it affects the decision of the respondents to participate in the research. Therefore, in this research, the anonymity of respondents was maintained throughout both the data analysis and the reporting of the results. The researcher chose to codify respondents with numbers, so as to be able to organise their responses and address their quotations in the discussion of findings. In accordance with the data protection act (1998), this research sought to use all information fairly, lawfully, and solely for the purpose that was stated. The collected information will be held responsibly and for no longer than the research enquires.

3.8.2 Level of Sensitivity

Cybersecurity and in particular, organisational management of cybersecurity is in nature, a sensitive topic. It is interrelated with competitiveness, reputation, compliance and might trigger thoughts regarding confidential processes, procedures, and information that many employees are not allowed to share or would not be willing to share. As the selection of participants is focused on those involved in the managerial positions, this issue might be heightened as they may feel responsible for managing and maintaining good practices within their daily jobs. To avoid any frictions and potential distress, every effort has been made to ensure no question required confidential information. All questions were designed to collect personal opinions regarding the concepts of cybersecurity within BIM-enabled FM, and only the general perception of their experience was of interest to the researcher. It was also made clear to the participants, that they are free to reject any question that they do not feel comfortable to discuss or for which do not wish to disclose information.

Taking into consideration the preliminary research findings, showcasing the poor management of cybersecurity within BIM-FM practices, the participants were assured that their answers would be solely used for the development of a framework to improve the current cybersecurity stance of the BIM-enabled FM industry and for encouraging cybersecurity-mindedness in digitalised organisations such as BIM-enabled facilities management.

3.9 Conclusion

This chapter presented discussions around the methodological decisions made by the researcher throughout the research process. For this purpose, the choice of research design, philosophical stance, research methods, techniques and tools were justified based on the discussion of various methods and views. The decision to employ an exploratory research approach to accomplish the research aims and objectives was made with respect to the nature of the study, research questions and the circumstances in which the research was conducted. The choice of critical realism as the philosophical stance enabled an exploratory study into BIM and cybersecurity, using the views and experiences of experts, together with rich knowledge collected from best-practice guidelines and standards, models, frameworks, and peer-reviewed journals. An inductive approach towards the research scope, coupled with qualitative methods of data collection and data analysis enabled the in-depth exploration of knowledge from various perspectives (Silverman, 2014). The chapter was finalised by the discussion of research quality and ethical considerations, to demonstrate the efforts of the researcher in the production of an authentic piece of work, with high academic values. This next chapter will present findings from the empirical data collection, using the research method discussed in this chapter.

Chapter Four: Empirical Findings- Interviews

4.1 Introduction

In fulfilling the third research objective, empirical data was collected through interviews, to expand and refine the primary research framework (figure 6). A detailed description of the methods used to design the interview questions, interview set-up and participant selection is presented in Chapter 3. Hence, this chapter presents the empirical findings, from the qualitative analysis of interviews and identification of the determinants of a cybersecure implementation of BIM in FM organisations.

Section 4.2 and its sub-sections demonstrate a structured description of themes extracted from the interviews, following the thematic coding of the interview transcripts. The identified themes (section 4.3) including BIM-FM determinants, cybersecurity determinants and challenges of cybersecurity integration in BIM-FM were divided into three subsections to showcase sub-themes pertaining to layers of strategy, implementation, and performance. The chapter concludes by providing an overview of the findings, later discussed in Chapter 5, to incorporate the results into the primary research framework.

4.2 Qualitative Data Analysis

4.2.1 Setup and Coding

The empirical data was collected following 25 interviews, which were transcribed and qualitatively analysed using thematic analysis as shown in figure 12.

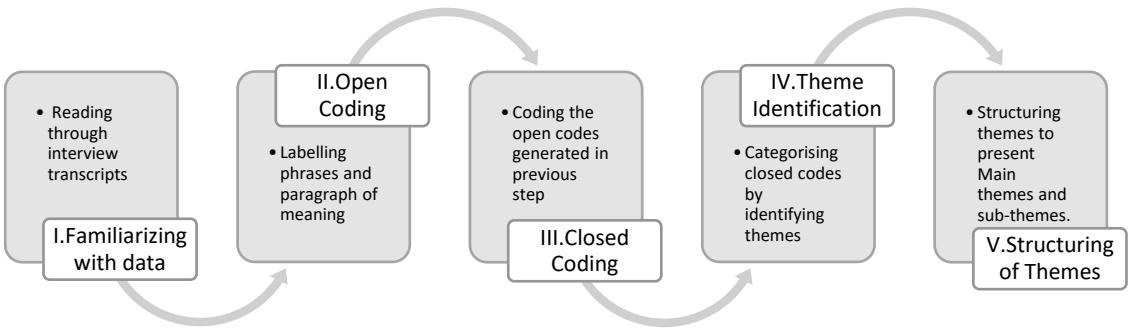


Figure 12- Data Analysis Process

The analysis started with: I. familiarising with the data; II. Open Coding; III. Closed Coding;

IV Theme identification, and V. Structuring themes (Figure 12). For the purpose of Coding, NVivo was selected as the qualitative data analysis software for coding and analysing data incorporated with the multiple contexts of BIM, Cybersecurity and FM. NVivo allows for an organised approach to the coding of high-volume texts and transcripts. Ignatow and Mihalcea, (2018) point to coding as a way of labelling data, which avoids repetition and allows for a more structured approach towards the interpretation of the data. Hence, the transcripts were thoroughly reviewed and open-coded to extract and structure meanings from the lengthy transcripts. Thematic analysis does not rely on the word-counts as it thrives to understand the core ideas that represent a theme (Guest *et al.*, 2014). A list of codes was produced as a result of applying the open-coding analysis to all 25 interview transcripts. The list was further narrowed down through closed-coding and constant comparison of codes with the quotes of the participants. The codes were abstracted from the transcripts to provide an insight into the practical challenges of the integration of cybersecurity in BIM-FM. Iterative closed-coding reveals overarching codes, contributing to the abstraction of themes which reflect the purpose of research.

4.2.2 Focus of interview questions

From a critical realist perspective, various parameters affect the way truth is captured and understood by its observer (Archer *et al.*, 2013). Therefore, the first three questions were structured to reflect on the profile of the participants, whose information included organisation sector, role and position and the area of facilities management for which they have experience of working. These questions enabled the justification and better understanding of the viewpoints of the participants gained through experience in various roles and organisations. .

The viewpoint and initial perception of the participants affect their observations of the facts (Archer, 2016; Groff, 2004). As highlighted in sections 2.2 and 2.4, there are various perceptions of BIM and cybersecurity, depending on the knowledge of the participant and their experience. The review of literature also demonstrated how various perceptions lead to different approaches in the management of cybersecurity and BIM. Therefore, questions 4 and 5 were added to capture the viewpoint of the participants on the BIM and cybersecurity phenomenon. This enabled the researcher to draw connections between the perceptions of the participants and their overview of the phenomenon and responses to other questions. Furthermore, considering the initial literature review findings (sections 2.2 and 2.4) regarding the one-sided views (due to over-reliance on the technology) around the multifaceted nature

(i.e., people, process, and technology) of both cybersecurity and BIM. Question 4 and 5 were designed to address this issue in a broad sense.

Questions 6 to 13 address the strategy, implementation, and performance levels in integration of cybersecurity in BIM-FM organisations. The questions were designed to address the primary research framework and seek new knowledge to enhance and tune the primary framework (See Appendix 3 for interview questions).

4.3 Thematic analysis results

Three themes of: I. Cybersecurity Determinants, II. BIM-FM Determinants and III. Inhibitors and Challenges of Integration emerged from the thematic analysis of transcripts. A synthesis of findings from the 25 interviews is presented in Figure 13 which illustrates the codes and the emerging themes and sub-themes.

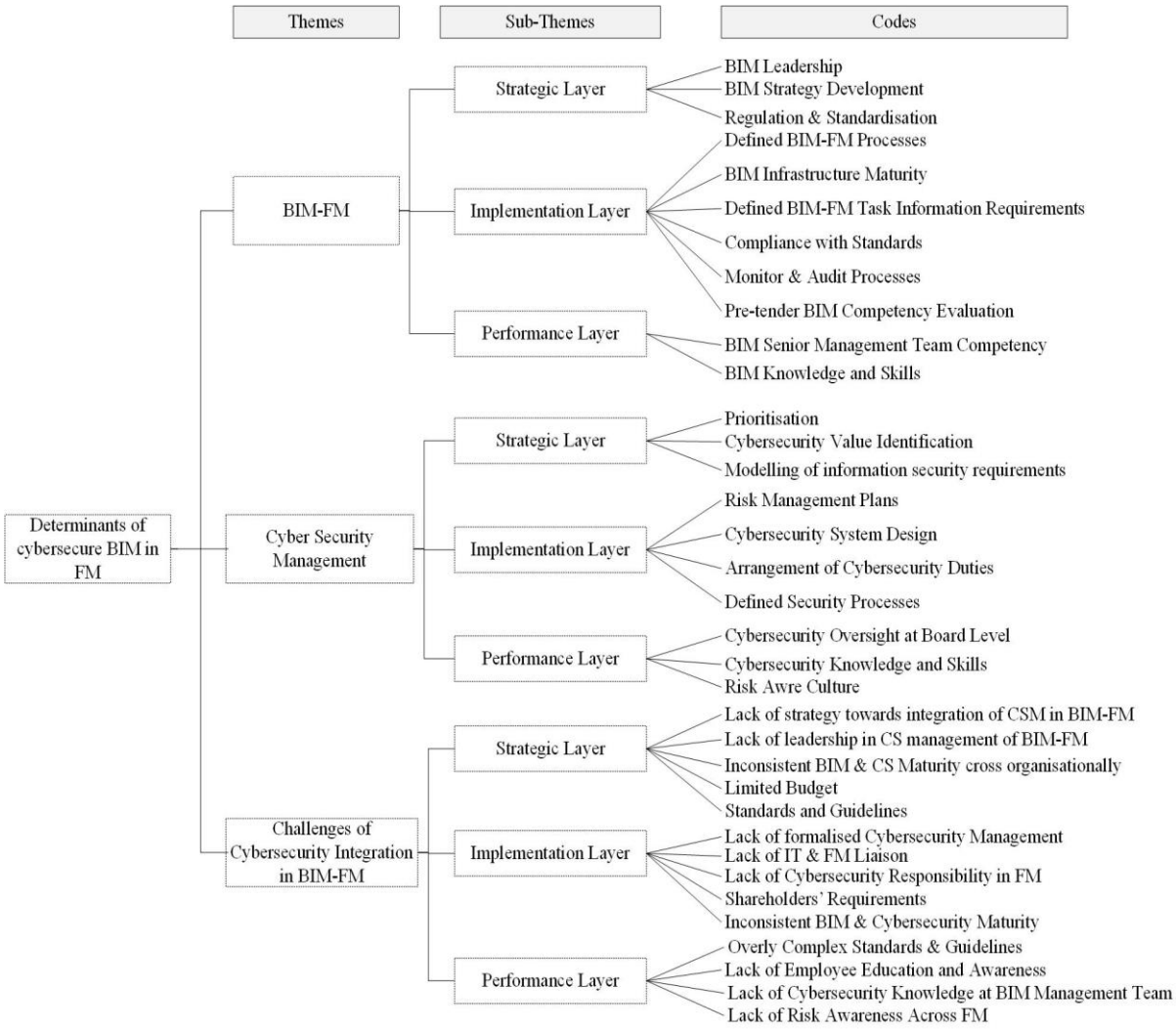


Figure 13- Interview Themes & Sub-themes

The figure presents an overview of the findings from the thematic analysis of empirical data. It illustrates the themes and sub-themes leading to the identification of the determinants that contribute to a cybersecure BIM implementation in FM. Sections 4.1.1 to 4.1.4 provide an insight into each theme, sub-theme, and their determinants. As evidence, interview respondent(s) who made comments leading to the statement made in the text is given (R followed by the respondent number).

4.3.1 General views of respondents on BIM and Cybersecurity

Questions 4 and 5 were only used as an indication of the general views of the respondents on the concepts to enable a better understanding of their responses to the questions.

4.3.1.1 Perception of Cybersecurity (Question 4)

Lack of a cybersecure culture in BIM-FM: Although 4 of the respondents believed that BIM-enablement of facility management organisations improve the cybersecurity of information, another 11 respondents pointed out an increased vulnerability brought about by BIM in FM. Also, 7 of the respondents agreed that BIM-FM organisations were behind the curve in the management of cybersecurity. The following statements support the above:

"I think the (FM) organisation are a little bit behind the curve in terms of data security."-R3

"A lot of people talk about cybersecurity, but very few people practice it."-R2

"I'm going to say, not very mature. I think facilities management it's been very much just get the job done whether it's within the individual areas of cleaning, catering, security, individual specialism if you like"-R4

Managing access to BIM data using CDEs: Although cybersecurity concerns were evident amongst the responses, 4 respondents pointed out that the information-management capabilities were enhanced by the use of CDEs. Particularly, they believed that the control and management of access to data made possible by such digital advancements was deemed as an effective method of maintaining the cybersecurity of data. In support of this view, one respondent claims:

"… in regular projects within the facilities management, data security would not be much of a problem as long as the systems in place are safe within CDEs and other spaces"-R17

Need for process to support technology: The level of trust of cybersecurity in digital tools differed between respondents. Whilst 4 respondents believed that CDE data-management

capabilities were sufficiently protecting data within a BIM project, 12 respondents strongly believed that working with CDEs and alternative digital tools required established processes and procedures to be in place, as well as certain knowledge, skills, and a level of awareness being required. Examples of statements were:

"I haven't seen cybersecurity prominently featured on any projects on BIM. User access to a common data environment and managing the password and multi-factor authentication are used but it doesn't seem to be particular to building the asset. It's just any kind of data and the need to know because of access regulations. So, I have not seen the 1192-part 5 standard being applied literally to a project yet."-R19

"When information becomes manageable from our end then there is another department which is called ISS. This information systems security department would look at how we manage different things, like servers, access to information and security."-R23

Data sensitivity depends on clients' requirements: As part of question 4 and depending on the overall nature of response, respondents were asked about their experience in dealing with sensitive data at any point in their jobs. 13 respondents touched on the information security requirements of the client from which 6 pointed out that government projects are usually the ones which require a higher level of security. Hence, the sensitivity of data is commonly defined by the clients and is project dependent. Examples of statements in support of the above were:

"Its simple things like floor planning and room number and things like that depending on the facility that you are at, and there would be a different security classification for managing that information"-R1

"I have worked in hospitals and there is a sensitive nature to some of the information about it …."-R3

"… The facility that you are at would have a different security classification to show how you manage that information"-R11

Lack of cybersecurity standards: 18 respondents have raised the issue of lack of a mandated approach to managing information security within digital facilities management. The following statement was one example:

"FM is still learning, and I think we are in a very good place in terms of being self-aware, but I think we need to get better. For example, I do a lot of work with the IWFM. We have only just

set up a technology special-interest group. We don't have a mandated approach for managing the information."-R3

4.3.1.2 Perception of BIM (Question 5)

Respondents expressed their views on a number of BIM features as well as a number of challenges associated with the adoption and implementation of BIM.

Information management aspect of BIM: The analysis of data demonstrated that 17 of the respondents were well aware of the information management capabilities of BIM and acknowledged the process of change associated with the adoption of BIM. In support of this, the following statements were made:

"To me BIM is a process it's not software. It's a process centred around an information model and that information model is not necessarily a 3D model it can be just data in a database. It's a collection of structured data, unstructured data, and 3D geometry and how you could collaborate together"-R11

"BIM is a combination of processes, people and different digital technologies to improve the way assets are designed, constructed and managed."-R23

Modelling aspect of BIM: Despite the above, 8 views were more focused on the modelling capabilities brought with BIM. As stated by the two respondents:

"It's a digital representation. I see it as software."-R16,
"Well by experience, using BIM is using technology you know, the advantage is to improve communication, avoid errors, to make things clearer and more organised." -R12

BIM benefits in FM: Respondents further acknowledged the benefits associated with the adoption of BIM in FM. An example of this was:

"….to ensure the most efficient (and that means in every sense of the word), management of the asset when in use, so whether it makes it more efficient in terms of energy, whether it makes it more efficient in terms of people and space, or in terms of cost, future maintenance and all

of those perspectives. So, it's putting all the right level of information together in the first instance so you can undertake that task effectively."-R5

Challenges of BIM in FM: 16 respondents have also touched on the issue of cost. The general belief is that there is a lack of investment in BIM implementations, and it is difficult to justify the upfront costs of the full adoption of BIM. In support of this, the following statements were made:

"the biggest hindrance is cost. It's the upfront cost which is the problem. If you look at the cost and the benefits over the longer term then it is justified of course, but the upfront cost is the issue."-R17

"… it's a very conservative attitude and no investments within facilities management, because it's all about keeping the cost to the minimum to manage the asset over its lifetime"-R19

The respondents' views on BIM illustrated a degree of understanding of the process change and culture shift associated with the adoption of BIM. However, the degree of understanding amongst industry professionals differ. Also, the understanding of the changes required for this digital transformation is inconsistent amongst the professionals. Most demonstrated a fair level of understanding of the benefits of adopting BIM, however, the challenges associated with implementing BIM in FM was also acknowledged (e.g., cost). Many respondents also affirmed the inconsistency in the way organisations approach the fulfilling of BIM requirements and pointed to the inconsistencies in BIM processes and procedures in organisations.

Findings from questions 4 and 5 were combined into the following themes.

4.3.2 Theme One: BIM-FM determinants

Theme one presents BIM-FM determinants identified from the thematic analysis of interviews. The sub-themes underpin strategic, implementation and performance related determinants, affecting the successful management of cybersecurity in BIM-FM. An overview of each sub-theme is described in the following sections. The empirical results showcase the relevance of each sub-theme throughout the analysis.

4.3.2.1 Sub-theme I: Strategic Determinants (BIM-FM)

This sub-theme highlights the strategic determinants, pertaining to the strategic competencies required within BIM-FM. The significance of developing a strategy for BIM-enabled facilities management was touched on by 22 of the respondents. As per the following statement:

"As soon as the management sets up the correct strategies, it means that everybody else which is procured will ultimately check the security box as well internally within the organisation"-R25

The competencies of top-level decision makers and their understanding and awareness in the management of BIM-FM play a significant role in BIM documentation, defining information requirements and quality of collaboration. Hence, it is interpreted that having a top-down approach towards the management of cybersecurity in BIM-FM is critical. The following respondent confirms this:

"*... how do the management and executives want to lead the supply chain to behave with that information. There are a lot of information requirements that need to be captured and documented on behalf of the client to enhance supply chain working. "-R13*

18 respondents have also pointed out the importance of considering cybersecurity within the requirements documentation. This is confirmed by the following statements:

"...what I expect from the client is what was formally called the employers information-requirements. So, what are they trying to achieve? what do they want? and how do they want information to be handled and managed? Without those in place, you kind of don't know what they are trying to achieve at their project"-R6

"... it (cybersecurity) should be in the organisational requirements, you know the OIR (Organisational Information Requirements), and it should feed all the way down through EIRs all the way through the BEP(BIM Execution Plan)."-R3

Almost all respondents pointed to the importance of developing a BIM strategy, which aligns with the organisational objectives. The following respondent adds to this by saying that there should be a success measure to work towards:

"Without a clear strategy no project would be successful. You need to work towards a certain goal."-R24

14 respondents further emphasised that a defined strategy acts as a reference for all BIM processes internally and externally. One example was:

"Obviously it would have been great if there were some sort of indications of a clear BIM strategy within FM organisations"-R9

In this regard, it was suggested that strategic planning should be dependent on the BIM lead. Hence, it can be interpreted that the quality of BIM leadership affects the success of strategies and consequently the overall success of a BIM project. As the following respondent comments:

"I'm not sure of any existing strategy plans. It would be more to do with the BIM lead. But everyone should have access to it I don't know if they are still working on it and that's why they have not shared it with us."-R12

It is also evident that the BIM lead is responsible for sharing and communicating strategies with all employees. This further affirms the importance of a top-down approach that feeds through all processes and procedures of the organisation. BIM standards and best practices are identified as an important determinant for the BIM-FM organisations. 7 respondents have demonstrated a customised approach towards the use of a combination of standards and guidelines. Examples of the comments of respondents are:

".. Because the PAS documents have been superseded by the ISO documents so we wrote our last EIR document when PAS was the standard at the time so within that document, we would refer to documents such as PAS555 secure cybersecurity. We also call upon other documents you know, such as ISO27001"-R23

"We comply with the ISO standards so we have our own approach to how we would talk to clients about BIM, but we are set out to deliver projects with compliance to those …"-R3

19 respondents have suggested that the BIM documents, such as the OIR, EIR, BEP and other requirements specifications should be developed based on the BIM standards and guidelines to ensure comprehensiveness and accuracy of content. One comment was:

"YES. ISO19650 part 1 &2. The PAS1192-5 is very good. It just needs a lot of linking to the BIM execution plan and the information requirements and the exchange information requirements of the asset, to help people manage the security requirement as well."-R7

Although not many respondents referred to any specific cybersecurity standards within BIM-FM, 5 of them pointed to the PAS1192-5 standard. An example of the responses states:

"PAS1192-5 is about implementing additional security protocols, so as you read through that, it is about assessing and applying different procedures in place so that would be possibly locking down your USB ports, or other procedures"-R6

Despite all available standards and guidelines, 19 respondents commented on the immature approach of FM in complying to those standards. In the light of this, one of them asserts that compliance would assist with improving processes and guides organisations towards an informed adoption of BIM for the FM:

"I believe all UK BIM documents and standards are very good, but the problem is people don't read or follow them …"-R15

4.3.2.2 Sub-Theme II. Implementation Determinants

This sub-theme demonstrates the determinants of BIM implementation that influence the management of cybersecurity within BIM-FM organisations. Responses to interview questions illustrated a number of these determinants. 20 respondents accentuated the critical importance of developing defined processes for BIM-enabled projects (i.e., BEP document). 14 have referred to documenting BIM processes and defining information requirements in accordance with the FM task requirements. One of them said:

"BIM documentations would be beneficial in terms of the information security objectives for the implementation plan. It's not common practice and it really depends on the organisations and the projects they are dealing with."-R14

Another respondent further elaborates by emphasising that effective collaboration requires an understanding of information requirements for FM tasks, and it is what makes a BIM project successful:

"The successful BIM project or digital project is something which is defined by collaboration and the quality of collaboration between the parties and that requires an intelligent client (FM

in this case). A client who is able to define the requirements in terms of the digital information needs and processes, is absolutely crucial to the success of the project"-R25

Examples of documentation within BIM-FM are mentioned by the following respondent:

"…the BEP can be used to either communicate initially what the client would expect to see in this space by the questions or the lay out of the BEP but certainly on the post-contract BEP, exactly how the supplier intends to work in this environment in a security minded way."-R13

Respondents have also commented on the positive implications of having defined BIM processes, on improved management of cybersecurity. One example was:

"…defining the processes is absolutely crucial to the success of the project. So as soon as the client sets it up the correct principles, it means that everybody else which is procured will ultimately check the security box as well internally within each organisation."-R25

Amongst respondents, 12 pointed out the variety of software, hardware and network systems used to enable BIM within a facilities management organisation. They indicated that the network solutions, CDEs and appropriate hardware and software is supplementary and project dependent. Hence, data exchange, access control and developing processes to support the operational tasks are identified and established on a client-dependent basis and between project stakeholders. One of them commented that:

"The diversity of infrastructure specifically the extent to which certain software or networking systems is used within the facilities management organisations is very much project-dependent."-R13

One respondent mentioned cost as another factor which contributes to the diversity and in most cases, acts as a restriction to the adoption of infrastructure required for BIM implementation.

"In terms of infrastructure facilitating BIM projects these are cost-driven, so it is really up to the budget available and the facilities management organisations are usually reluctant towards full implementation of cloud-based systems"-R14

Despite the comments above, 10 respondents specified the need for a well-managed and

strategic approach towards BIM infrastructure. In particular, one of them pointed towards the use of CDEs and cloud-based communication, and the benefits associated with it in terms of enabling easier management of information security:

"We are now taking measures to launch our own systems and own the data from start to finish. So, we procure through a common data environment system. I'm responsible for setting up the user groups to ensure everything is secure and share only with the people who need it"-R7

The importance of having a responsible body who manages and monitors the infrastructure and digital platforms was raised by one respondent:

"Typically, the idea of the project team working on a single platform, which in most cases its either BIM 360 or Aconex, has to be a single platform maintained and managed by somebody, and that somebody is appointed either by the client or by the principal agent, as being the empowering body, the appointing party."-R16

Amongst the respondents implementing a more mature approach towards BIM infrastructure through using CDEs and their underlying processes, security concern was prominent. 14 respondents also touched on the access to data provisions as well as the control and management of information exchanged through CDEs. However, the success of managing the cybersecurity of data depends on the solution that is implemented to address this issue. Although maturity in BIM infrastructure facilitates the adoption of advanced technical cybersecurity solutions, it will not guarantee a successful management of cybersecurity. Respondents have expressed their concern about the insecurities within digital platforms and systems:

"The other issue is the insecure architecture of some of the common data environments and some of the CAFM systems."-R1.

"I think that there is a perception that if the data sits on the supplier system and it doesn't interact with the client system, then it should be okay. But when you get to check that, you find that the supplier system is actually having to hold on to sensitive data whether it be credit card transactions, or even names, you know, it's a big challenge."-R24

One of the regularly occurring themes identified by the respondents was the need to identify and document project information requirements within facilities management. 19 respondents indicated that by defining the project information-requirements for FM tasks within the BIM process, the documentation would help to improve efficiency in organisational working-processes, both in terms of time and cost. As one comment highlighted:

"…if you could have put security protocol within there it will only give you the information that is relevant to you, so therefore you're going to spend less time and money searching for data that necessarily doesn't have anything to do with you. It's good in two cases"-R9

One respondent affirmed that, by emphasising that to be able to secure the information, organisations should identify which information is required and which stakeholders should undertake a certain task:

"…you need to be able to secure a data base but keep it free to the people who need to know it and are assigned to know it."-R19

Respondents also argued that having project information requirements identified, managed, and documented, leads to organised and well-structured information management processes. Some have also pointed to the effects of this determinant on managing the security of information, by giving a clear indication of who needs to see what. An example of one of these responses was:

"…you do not need to worry about the security of that information as long as you are being pretty restrictive about you only need to know what you need to know… that depends on the service and what you are asking them to do."-R18

Across all respondents, compliance with BIM standards and guidelines was described as challenging, yet beneficial. 6 respondents expressed a lack of knowledge the contents included within BIM standards and guidelines. They assumed that their organisation complies with best-practice guidelines and standards but were not informed of the details. As one respondent comments:

"Yes, we certainly do (comply with standards) and I think it's very beneficial. I'm not so close to the standards so I can't say off the top of my head. I have not really been heavily involved in using the standards that common. So, yeah, at this point I'm not sure."-R21

On the contrary, there were 7 well-informed respondents who claimed that their organisation was in compliance with the British Standards (BS), PAS suite and/or ISO standards. Examples of such responses was:

"YES. ISO19650 part 1 &2. The PAS1192-5 is very good. It just needs a lot of linking to the BIM execution plan and the information requirements and the exchange information requirements of the asset, to help people manage the security requirement as well."-R7

There is a difference between the respondents whose organisations complied with standards and those who were not mature in terms of their compliance status. The compliant organisations were more likely to develop structured processes for the management of information. Also, they were more likely to consider the cybersecurity of data as an important aspect of information management. Although some argued that the standards and guidelines were overly abstract in some instances, there was still a consensus on the benefits of compliance. As demonstrated by the following comment:

"…being in compliance with those standards will provide a better cyber security status for 90% of the projects within facilities management. But the problem is they don't tell what should be done so they assume the person who is doing the security knows what he is securing…"-R22

Interviews also revealed that education was required to facilitate compliance. The comments of respondents exemplified that the regulatory bodies in charge of developing the standards had failed to engage industry in the development process and hence, those standards were missing examples and practical insights. Hence, industry was failing to understand the applicability of the content. One comment was:

"I think that we are very naïve in that world, but I think the fault is with the industry. I think it is the fault of two areas. One is CPNI and the people who wrote part 5 because they didn't make it consumable enough with examples and this is the fault of UK BIM Alliance for not

engaging properly in the educational world…we go back to the original BIM where there was place for engaging education and they failed to educate people in part 5."-R9

Although standardisation at strategy level was deemed critical, the extent of applicability to practice was argued by some respondents. One of them claimed that in some cases, strategies are standardised but there is insufficient guidance as to the way in which compliance can be achieved in the implementation and execution:

"You know the PAS1192-5 was labelled as optional which should have really been made compulsory. You know that although something is included in the EIR, it's just lightly touched on, which is not sufficient for the appointment documentation! It should be clear what each organisation needs to do to be in compliance with the standards and best practice guidelines."-R25

18 of the respondents pointed to the audit trails and monitoring processes. However, the differences were in the type and target of assessments. 11 of them commented on the importance of audits for improving processes to achieve a higher performance. One said:

"Auditing processes are the only way of somehow assessing the overall performance of the organisations and improve the processes according to the outcome"-R24

Amongst these respondents, 7 have commented on the importance of both auditing and monitoring. Responses around auditing are commonly linked with checking compliance to organisational rules and regulations as well as best practice guidelines and standards. In contrast, 5 participants pointed instead to a quality check which is project-dependent and is carried out to check if the project requirements are met. Hence, the target can include performance quality or output product quality. Both have been proposed by respondents as critical to maintain and improve effective organisational strategies and processes. Two of the comments were:

"… as long as it's being audited to ensure they are actually carrying out what ever those duties are according to project requirements, I assume that should be a good approach."-R10

"Yes, there is, we get audited at every quarter and it (cybersecurity) should be something that's picked up every time, I can't say if it is, so we have an external company that used to do it…they are auditing the projects that we are working on, are in compliance with company policies, and if applicable, ISO standards statuary requirements etc. etc."-R3

Furthermore, the monitoring processes, particularly the data handling processes including data exchange, access and archive processes were pointed out by the respondents. 7 of them stressed that monitoring enables protection against cybersecurity vulnerabilities and provides an insight into the processes and procedures in need of revision and improvement. Two of them commented:

"We have robust data exchange processes. Our data security team is monitoring every aspect of data security within BIM projects. Of course, there is always room for improvement."-R13

"Probably a good record of the historical data and the history of movement and where things are going. A good tracking of every movement within that environment so that if something changes or something disappears, they know why and who has done it or if someone has added a file, just know who and when that has been done."-R12

BIM-FM entails tendering with various stakeholders contributing to the project. 16 respondents have raised concerns regarding the inconsistencies across organisations. Particularly, the variety of information management and data-handling practices were identified as affecting the quality of collaboration within BIM project stakeholders. They proposed an evaluation of capabilities, competencies, and processes of the stakeholders at the pre-tendering stage. It was also suggested that certification would demonstrate their capabilities, however, there still needs to be evaluation procedures to ensure processes and procedures are in line with both organisational and project requirements. One comment was:

"The facilities management should have some sort of a standard in tendering so they should really look at the security levels of the stakeholders and assess them against the security requirements of the project. This in itself requires a broad understanding of what needs to be done, which I believe the available guidance docs demonstrate very clearly"-R4

Another respondent further points to the alignment to ISO27001 when evaluating the competencies and capabilities of stakeholders:

"I think it's important that when we issue an invitation to tender an ITT to the design team, we issue a supply chain capability summary document and the section in there on information security and management and we would expect our design teams to have a knowledge or even better certification aligned to documents such as ISO27001 so we would ask them a number of questions aimed at how the design team could aim to ensure that project information is secure all the times."-R23

4.3.2.1 Sub-Theme III. Performance Determinants

This sub-theme pertains to the social and people related BIM determinants which affect the successful management of cybersecurity within a BIM-FM organisation. Both concepts of BIM and cybersecurity entail socio-technical factors which facilitate the execution of implementation plans and the achievement of strategic goals.

In light of the above, respondents have pointed to a number of capabilities required by the BIM management team which enables the cybersecure leadership and management of BIM. Examples include the competency of the management team in assigning roles and responsibilities to the right individuals and teams. As one comment showed:

"… but ultimately there is a responsibility on whoever that is appointed to that job to do that with a level of competency, and you know who I am appointing to do that you know it's my competency as the member of the executive"-R1

Furthermore, respondents have indicated that the management support when implementing BIM, in terms of resource allocation entailing budget and human resources, affects the cybersecurity management capabilities of the organisation. Hence, it was proposed by one respondent that there needs to be an allocation of budget to provide suitable infrastructure (e.g., software, hardware, and networking systems) to facilitate the achievement of optimum benefits of BIM within the FM organisations.

"In terms of the maturity of infrastructure facilitating BIM projects these are cost driven, so it is really up to the budget available and the facilities management organisations are usually reluctant to support a full implementation of cloud-based systems"-R14

Affirming this point, another respondent commented:

"Again, every decision is cost driven within the FM world. Not much consideration apart from the cost is put into the selection and purchase of infrastructure. The maintenance procedures follow a similar trend"-R6

Another respondent comments on the importance of training and education in using infrastructure that facilitate BIM:

"I think if you have everything locked, we go through this with clients all the time, they say I need to use this system and we say well this is how it's going to be used and structured and we should train you to be able to use it correctly"-R19

It was also indicated by 9 of the respondents that understanding the roles and responsibilities required for managing a cybersecure BIM project is important for implementing a top-down approach to achieve a security-minded BIM implementation in FM. Hence, the need to comply with standards and best-practice guidelines have been mentioned by some respondents. One of the comments was:

"… the responsibilities set out in part 5 are pretty clear, and that is, you need to think about what is it that you are trying to do and set out what you are going to do for any job stages. Even if that's the case then we just need to ensure that somebody confident is appointed to that role, such as the built-asset security strategy manager."-R1

All respondents have referred to the need for BIM knowledge and skills, including the ability to work with BIM authoring tools and to understand BIM models used for FM purposes. It has been pointed out by the respondents that in fact, many FM organisations are yet to be trained to benefit from BIM in the in-use stage of a facility. The discussions around BIM knowledge and skills also necessitates an understanding of FM data requirements. A comment in supporting of this view was:

"The issue with the construction industry as a whole, is that they rush into digital ways of working without realising what it takes to fully achieve the benefits. So, with BIM, there are many organisations who claim they do BIM, but their performance is poor due to their lack of awareness, knowledge and skills."-R4

The comments of respondents exemplified the positive impacts of BIM knowledge and skills on the cybersecurity of project information. Where the knowledge and skills pertain to the ability to manipulate and understand BIM models and authoring tools, it leads to the right modelling procedures such as the production of layered models. Respondents argued that in this way, various views can be shared with different stakeholders according to the task information-requirements. Hence, only essential information is shared. As commented by one respondent:

"When we first got BIM, we were sort of under the impression that a BIM model is going to be one model, not multiple models' kind of stitched together. You know in a big hospital you might have zones of BIM models, but I think within an MEP model and a finishes model, maybe there is a lot of information which really need structuring and layering to be able to efficiently collaborate with the other parties securely."-R20

For 9 respondents, BIM knowledge and skills entailed the understanding of BIM processes and acknowledging the potential advantages of BIM for managing project information. They believed that this would lead to BIM projects that are carried out in compliance with the standards and guidelines that operate through the development of the right information requirement documents such as EIR, OIR, etc. 12 respondents also acknowledged that the development of accurate information-requirement documents significantly benefits the cybersecurity of project information. One comment was:

"BIM within facilities management is only beneficial if there is valid data available which can be managed and if the facilities management team know which data is required for which task. Then there can be some sort of use of BIM capabilities but if the data is not there then facilities management would have a hard time just to get that data. The use of BIM across the facilities management team is very scarce and it is not quite clear, what the requirements are for successful BIM projects"-R16

Furthermore, another respondent emphasises the importance of understanding both BIM models and information management processes in BIM by stating that:

"Unfortunately, what BIM is understood as it a way of doing projects but in technical terms. So, when BIM is stated, it is usually about having a pretty 3D model which represents the building or the facility. So, what is not taken into consideration are the skills for modelling and design. The information-management aspect of BIM projects is still poorly performed. The value of BIM is not fully captured within the facilities management organisations due to the poor adoption of BIM capabilities."-R15

11 respondents have further indicated that BIM Knowledge pertains to the understanding of what is required for implementing a mature BIM in an FM organisation. This view is more inclined towards the managerial positions who decide the processes, responsibility assignments, budget, and human resources. In this regard, knowledge, and awareness of risks, particularly at higher organisational levels and where the strategic decisions are made, is also taken into consideration by the respondents. One of them commented:

"..., they do essential training, like awareness training which everybody needs to do, understanding what the environment is like and where the potential is for these, but there is definitely a requirement for focusing on particular roles. This should be not many though, essentially just executive management, the lead design position, the BIM user and then finally the administrative staff. So just basically for the sense of information, you've got decisions being made at one level but there are executive decisions at a higher level, and each of those should have a bit more focus on what the potential risks of decisions at that particular level were."-R14

Whilst BIM knowledge and skills are found to be essential for the adoption and implementation of BIM within FM, it is also argued that successful implementation of BIM within FM requires continuous improvement of knowledge and skills. 19 respondents insist on continuous training and argue that it is one of the key enablers of process improvement. One of the comments was:

"I guess training would be the best thing that can be done because there needs to be some sort of an educational course for staff, and it needs to start from baseline but as we get better it

needs to be more focused and more detailed. Because the thing is technology is improving every day and it is changing every day so there needs to be an ongoing training session for everyone to keep up to date with the things, they need to know about the technologies they use as part of their jobs."-R12

4.3.3 Theme Two: Cybersecurity Determinants

Theme two also contributes to addressing the second research objective, by investigating the determinants contributing to the achievement of cybersecurity in BIM-FM organisations. The sub-themes address determinants for the strategy, implementation, and performance layers of BIM-FM. This approach assists with maintaining consistency with the primary research framework proposed in Chapter 2. An overview of each sub-theme is described in the following sections. The empirical results showcase the relevance of each sub-theme throughout the analysis.

4.3.3.1 Sub-Theme I: Strategic Determinants

This sub-theme demonstrates the strategic determinants, pertaining to the strategic determinants for cybersecurity, applicable to BIM-FM.

Amongst most respondents, the prioritisation of cybersecurity management within BIM-FM organisations was a matter of concern. The respondents argued that the modus operandi of facilities management organisations is overly cost-driven, and the focus is on "getting the job done". They also commented on the effects of this on the quality of processes and procedures, particularly within a BIM-FM project which requires sufficient technological, financial, and human resources. Examples of comments were:

"….it would have been great if there were some sort of a clear strategy but unfortunately Facilities Management organisations are not focused on this. The priority is with getting the job done with minimum cost."-R9

"…I think part of the problem is that your data security is so often not as high on your priorities list that probably should be."-R1

Respondents further indicated that an immature approach to BIM currently exists amongst many stakeholders who are solely focused on the modelling capabilities of their digital

infrastructure, whilst overlooking cybersecurity considerations during their operation. As the following comment shows:

"…I would then look at what systems solutions software etc are going to be used throughout the BIM project, but we kind of go one step further, in terms of, you know, the client is probably more interested in the capability of that software and how that capability will actually bring benefit to the client or the asset or the project. I am also focused on where that solution is hosted, does it need penetration testing, is it cloud based? Do we need to visit the data centre etc, etc."- R13

Value identification was captured from the responses of the respondents as an influential BIM-FM determinant, supporting better strategic decision making. As the following comment illustrates:

"I don't think we as a business have really sort of thought about the value of it and how we should be securing the model in terms of what information should be shared, who can see what, etc."-R1

The respondents also touched on the importance of a balanced approach towards the management of cybersecurity. There was a consensus that the cybersecurity strategy must not jeopardise organisational operations. Hence, the value identification was essential to ensure the cybersecurity strategies are aligned with the goals and objectives of the organisation. Respondents comments, on identifying the values created by implementing cybersecurity risk management strategies, support these points:

"….and therefore, how you derive value for the organisation, so you need to keep the transparency to a level! you don't want the operations to be disrupted or awfully complicated due to security measures."-R4

"…its actually quite difficult to get across the convincing business case to do it. I am doing some of that now. Where we are trying to say to people that we know this is the right way and the right direction to travel, but the CFO will say well how much is it going to save me? That's quite difficult to answer! Because we don't know what the answer is in pounds and pence."-R3

Furthermore, modelling organisational security requirements has also been identified as an essential capability for the cybersecurity leadership team. Respondents have pointed towards the importance of considering the cybersecurity requirements, with respect to their collaboration processes and procedures. As the following respondent comments:
"FM companies should really improve their cybersecurity scope and how they manage the cybersecurity issues as a business not just for specific projects. I think if FM companies got the right processes and procedures to meet their security requirements, then
that would automatically follow for a BIM perspective..."-R20

Respondents particularly point towards understanding the cybersecurity risks against the organisational business goals. An interpretation of such statements stimulates the organisational risk appetite and have an impact on security requirements modelling. Some organisations might face less cybersecurity threats due to the nature of their work, however, others may face severe loss as a result of a cyber-attack. Therefore, the risks should be identified and the extent to which the organisation can absorb the risk should be determined. As mentioned by the following respondent:

"... I used to work for a very small consultancy for which there is not much cybersecurity risk you need to worry about in that. I worked for another company and they had a security section in the basement where you need a special key to get through their front door..."-R14

Respondents have also pointed to the standards and guidelines as a determinant influencing the cybersecurity management strategy within BIM-FM organisations. The comments of respondents entailed compliance with a variety of standards in the domains of BIM (e.g., PAS suite) and information security (e.g., ISO 270001):

"...if the data is sensitive then the PAS1192-5 standard should be used. Now that standard has been converted to an ISO standard at the moment so should be available as an ISO standard maybe this year or later."-R1

"...we have ISO270001 and that kind of thing which just means that we are up-to-date with the latest security standards in terms of the data."-R16

Whilst respondents insisted on the importance of compliance within FM practices, they were heavily reliant on IT teams or technology providers and were lacking the cybersecurity in their FM processes and procedures. As the following respondents commented:

"… in general, most projects promise a data security point of view which is making sure that the common data environment is being proposed from a reputable company that follows proper standards for their data centres and they rely I suppose on the providers of those systems to be secure in the data."-R15

"…Perhaps to a certain extent, security is someone else's problem, so it's not even considered in an environment like a BIM model"-R10

Although respondents claimed to have robust processes for the exchange of digital data in compliance with the best-practice guidelines and standards, they also pointed to the barriers and complications associated with maintaining compliance in the multi-stakeholder nature of BIM projects. In light of this, one respondent pointed out the diverse range of standards which cause inconsistency in BIM projects which involve multiple stakeholders globally.

"…there is a complete lack of standards even though they are a number of standards available. It's the diversity of standards which potentially causes major issues. There are American standards, UK standards, some of the European standards, Middle East standards and the Far East standards for instance…"-R14

Another respondent also elaborates on the barriers of compliance by indicating to the divergent capabilities and characteristics of stakeholders involved:

"PAS1192-5 is about implementing additional security protocols so as you read that that is about assessing and applying different procedures in place so that would be possibly locking down your USB ports, or other procedures. We do look at it but unfortunately the nature of the clients that we work with, are not grasping the common data environment fully yet so we still need to have some of that open"-R6

In addition to the aforementioned determinants, financial resources appear to be one of the key determinants of a successful management of cybersecurity within the FM industry.

Respondents commented on the cost driven nature of FM practices and emphasised that the facilities management organisations are more focused on cost efficiency than improving cybersecurity. One of the comments received was:

"When you remove something like cost then you can discuss other things because for getting all the data you need in all that formats and doing all those stuff costs a lot and it's the first barrier that you need to cross and I'm sure there are other things that you need to value as you remove barriers, but the main issue is cost effort and time! It's those three things."-R8

Furthermore, respondents proposed that value identification can encourage budget allocation for cybersecurity considerations. They also suggested that the competence of the BIM leadership, entailing risk awareness amongst the management team is an important factor in understanding the long-term gains of investing in cybersecurity best practices within BIM-FM. In this respect, one respondent comments:

"so, the way that I would handle it, is to first brief everyone where the problem lies, to make sure that people are aware, that it isn't just a case of dealing with cybersecurity. It isn't just a case of dealing with physical security. You have to be persistent to make sure it's a combination of all those things that need to be in place for the right approach to managing security and therefore the level of understanding needs to be broadcasted, advised, top to bottom. Any new-starter inductions need to take place, so everyone is aware of how that a security-minded approach flows from top to bottom in that organisation."-R11

4.3.3.2 Sub-Theme II: Implementational Determinants

This sub-theme demonstrates the cybersecurity determinants that benefit BIM-FM organisations in implementing cybersecure BIM practices. By integrating cybersecurity determinants in BIM implementation, the structures and competencies will have cybersecurity at their core. Hence, an organisation achieves a seamless integration of cybersecurity within its plans, processes, and procedures.

Considering the above, respondents discussed the organisational approach towards cybersecurity risk-management. Many respondents claimed that their risk-management plans do not include cybersecurity:

"…we have a risk management plan, it includes all the health and safety aspects, but it does not touch on information security I don't believe it does."-R17

"The facilities management to my knowledge don't have such thing as cybersecurity or information security risk management maybe they have the risk-assessment briefings and tick boxes to make sure that its safe but not to my knowledge."-R25

Whilst 19 respondents believed that including cybersecurity in the risk assessment of BIM-FM is critical, 6 respondents did not consider it as part of the role of facilities management. One of the respondents mentioned:

"BIM is a software tool a digital tool or a database what-ever you want to call it, so, yeah, it's IT/IS functionality I think to control the access"-R20

Respondents claimed that the cybersecurity risk-management plans are solely focused on the CDE or systems cybersecurity. As one of them commented:

"That's got to be organisation by organisation, so as a prime organisation you would do cybersecurity-risk assessment on the software or hardware that you are thinking of procuring."-R24

Respondents also pointed out the need for identification of the level of sensitivity for various data within BIM-FM. They believed that identifying the risks associated with different groups of data was critical for the information-security management and can further ease the data access permits. As one participant indicated:

"… a risk assessment is carried out, then following that would be the realisation of what level of security is required for the systems, the hardware, the software, and who can see what, as I said earlier. So, the need-to-know basis would highly depend on the results of the risk assessment."-R19

Respondents also discussed the lack of risk-management plans across the FM organisations. Financial and human resource limitations and other challenges such as a lack of risk-aware decision making at the senior management level has resulted in discrepancies in the risk-

management approaches. Responses expressed positive views on the establishing of a cybersecurity risk-management plan and further stated that it should be a shared responsibility between technical and non-technical departments of an FM organisation. A comment by one of them declared:

"The problem I see is allocating resources to that, so it's another undertaking that would probably need a little more collaboration between our own security department, but at the moment it probably hasn't happened to the degree that it needed to. "-R23

13 respondents also considered that the cybersecurity design of systems was a very important determinant in the successful management of cybersecurity in BIM-FM. They expressed the view that cybersecurity should be integrated within the processes to ease everyday working tasks rather than adding an extra pressure on staff. Hence, an effective cybersecurity design for systems can facilitate an easier integration. 20 of respondents pointed to the system access permits designed for CDEs used within BIM-enabled projects as an example of cybersecurity design for systems. As one participant said:
"…we are now taking measures to launch our own systems and own the data from start to finish. So, procure through a common data environment system. I'm responsible for setting up the user groups to ensure everything is secure and shared only with the people who need it"-R7

Respondents believed that the technological integrity and reliability of the cybersecurity systems were important and pointed that an optimum design of such systems cannot be achieved without the collaboration of IT and FM teams. As exemplified in the following comment:

"… there is a lot of collaboration between what the IT team you know understands, and the people who understand the operation, so that they could somehow work together to find the best solution."-R21

Respondents expressed divisive opinions regarding cybersecurity accountability across the BIM-FM organisations. It was shown that the responsible body is labelled as information manager, BIM manager, information security manager, etc. and requires a different set of

competencies compared to typical BIM managers or project managers. Some statements from respondents supporting these points follow:

"… the appointment of an information manager is really critical to the move to the CDE in BM. It's not something that you can leave to a single BIM manager who is responsible for only one discipline. This needs to be somebody who has a better idea for the project management, risk assessments, the legal and contractual arrangements all of which in most cases exceeds the bounds of the typical role of a BIM manager, so it would be a person who would be appointed specifically to manage that aspect of the documentation. That is rather a particular and more specific task."-R14

Respondents also referred to the BIM guidance documents and standards (e.g., PAS1192-5), with one of them proposing the assignment of a built-asset security strategy manager.

"…we just need to ensure that somebody confident is appointed to the role of built-asset security strategy manager."-R1

Alternatively, respondents also believed that there was a lack of knowledge and skills across the FM teams for involvement in cybersecurity-related duties. Hence, this responsibility was solely assigned to the IT teams and/or system providers.

"I believe the responsibility is lost within the organisations and specifically with the facilities management, there is extreme lack of processes and lack of knowledge in terms of monitoring cybersecurity of data. The responsibility should be with the information manager or the project manager, whatever it's called, but there should be someone responsible."-R24

"… it should be the facilities management team, for every asset we are talking about and that it is up to them to ensure that the platform they are using is providing them with an adequate service and that should be fairly well scoped in terms of agreement with the software provider …."-R2

The silo approach was criticised by 4 respondents, shedding light on the knowledge and awareness shortfalls. In this regard, respondents explained that the IT teams lacked the necessary awareness of the FM information requirements and data sensitivity levels, whilst the

FM team lacked an awareness of the systems vulnerabilities and technical cybersecurity-solutions. Hence, it is suggested there is a need to have robust processes for both departments and to have effective communications and collaborations in the management of cybersecurity:

"I believe the IT department within the university or the main client organisation usually takes on cybersecurity which I don't think is sufficient to fully take care of the cybersecurity complications that might arise in FM."-R25

" the only way it is going to work is by a collaboration between the technical geeks and FM geeks, but the problem is to find a common language for both of them to use so they understand what they are saying to each other, which is going to be a challenge…."-R22

Furthermore, respondents indicated that a top-down approach was an effective way of ensuring cybersecurity is fed into all processes and procedures. However, successful cybersecurity management will not be accomplished without a security-minded culture and that requires sufficient knowledge, skills, and awareness for all employees within FM:

"I don't think it's necessary for every team to have like an individual who is the cyber guy! that to me is to me probably unaffordable and you don't integrate that cyber-awareness and knowledge into the team"-R19

"It's up to the users to ensure the work they do with software or their use of the devices is executed in a secure manner. But also, they need to know how to perform securely. Each software and each device or let's say different common data environments require certain considerations to be taken into account. "-R3

Respondents were questioned on the data-exchange processes, including access and storage of information in a BIM-enabled project. They argued that the client's requirements play a key role in the processes and procedures. This is particularly related to the maturity of the client in the understanding of BIM infrastructure and financial affordability. As noted in one comment:

"The reason is underinvestment and people in senior levels not understanding the importance of cybersecurity I think and its often very fragmented you know…things can go very wrong if you don't have a top to bottom security-minded approach."-R11

Respondents stated that many clients have not yet adopted a CDE and hence, collaboration procedures will differ to the ones who have one and have sufficiently invested in BIM infrastructure.

"PAS1192-5 is about implementing additional security protocols so as you read through that that is about assessing and applying different procedures in place so that would be possibly locking down your USB ports, or other procedures, we do look at it but unfortunately the nature of the clients that we work with, are not grasping common data environment fully yet so we still need to have some of that (security protocols) open but we do have some practices in place…"-R6

Respondents have also claimed that each organisation has its own ways of working. Furthermore, the organisation-specific regulations commonly incur contradictions and restrict collaboration. As one respondent indicated:

"It depends on the client and it depends on the asset, so I work with a lot of clients across all different sectors with different levels of security and what that security means, is it around the design of the asset, is it around the operation of what that asset is going to physically do, is it around the output of the asset i.e., smart manufacturing you know lots of intellectual property etc etc."-R13

The comments of the respondents illustrate a lack of defined processes across FM organisations which leads to prejudice of the cybersecurity within digital data exchange and archive processes. As one respondent comments:

"Information Security is indeed an unpopular topic in the facilities management organisations. Of course, it is dependent on the projects and clients and if for them, information security is a matter of concern, then there would be measures to ensure security from multiple aspects."-R15

4.3.3.3 Sub-Theme III: Cybersecurity Performance Determinants

This sub-theme presents the determinants that contribute to a cybersecure performance amongst professionals working in BIM-FM organisations.

Both concepts of BIM and cybersecurity entail socio-technical factors which facilitate the execution of implementation plans and the achievement of strategic goals. Amongst these factors, 14 of the respondents agreed about the importance of management-team competencies in cybersecurity. Respondents believed that cybersecurity oversight at board level will feed into all processes and procedures. The following comments exemplified this:

"There needs to be that consciousness of the importance of cybersecurity and that it needs to be applied to every task. For people to see it as important as the data itself. There should be a top-down approach because if it starts with the top then it would easily cascade down"-R21

"... Clear and open protocols of risk assessment need to be implemented along with the training and understanding of what the cyber threats are, because the majority of the facilities managers may be familiar with the concepts on a very generic basis, but they wouldn't be very technically savvy. They need to have explained to them how the digital information transformation would be risky and how they should manage the security of that system and they need to have the guidance document which would guide them through how they can successfully maintain security knowing the vulnerabilities and risks."-R2

"There needs to be appointment at executive level with a clear set of responsibilities ultimately for everybody appointed to do any job then if they are incompetent to do it or if they are not doing their job probably, they should be sacked."-R1

Additionally, knowledge and skills are identified as a major enabler in implementing a cybersecure BIM within an FM organisation. Respondents have raised concerns regarding the lack of cybersecurity knowledge and skills amongst non-technical FM professionals. The following respondents further illustrated the importance of training and educational programs for all FM professionals who are involved in a BIM-enabled project.

"There is lack of knowledge and awareness which is not only within the facility management sector, but also across all industry. ... So, they are producing digital data but in general they print it up or they make it a pdf. The exchange of information has always been through

something static that you know rather than data exchange. In general, there is a lack of knowledge and skill about the data exchanges."-R15

"I think the challenge comes back to that naivety and the fact that people don't quite understand how to do it and what to do. And they need to have a lot more education a lot more examples and guidance to help them to do that."-R9

As the FM industry is evolving from the traditional ways of working to a digital modus operandi, FM employees need to improve on their technical proficiencies. Technology is becoming part of the everyday working-procedures and professionals need to be aware of the challenges and vulnerabilities of technology-enabled working environments. Respondents have demonstrated that integrating cybersecurity within the strategies and work processes will only succeed if employees are sufficiently competent to follow the instructions and practice cybersecurity in their day-to-day job. The following respondent emphasises the need for training:

"…and the problem there, is that once you say, yes, everybody has got to be on here (centralised system) is that everybody has got to be trained."-R18

Respondents have also indicated that a cybersecure BIM within facilities management organisations requires a change of mindset and a shift in the organisational culture. This entails the transformation of views and commitments and values and is deemed essential for a successful execution of strategies and processes. 18 respondents agreed that facilities management employees were not willing to get involved in the cybersecurity considerations and did not make efforts to improve their technical skillset. This is further demonstrated by the following respondent who says that FM professionals believe that the IT team and system providers can fully protect the data from any cyber threat.

"I think it is not in the top priorities for our job. We have an IT department who look after all data and security stuff, so I don't see any point in that."-R17

Another respondent further emphasises the need for a culture change by stating that:

"…what I have observed is people are obviously more willing to pay money for a new system, but they find it much harder to change behaviours and that itself is a large investment. To make people do things differently is what is required. So, paying for a new technology is just the tip of the iceberg."-R19

Interviewees also commented on the lack of internal collaboration and communication amongst various facilities management departments. This was interpreted from some responses as relating to the processes and procedures, in which the respondents were unaware of the common procedures or regulations of the organisation:

"I can't comment on that. I'm sure there are rules, but I have not been exposed to them. I probably haven't been within the right environment to have that exposure, where I would pick up that information."-R21

"…as far as I am aware, some sort of a risk assessment was done a while ago maybe something was communicated but I don't remember. But it's certainly not recommunicated and not updated, and I think cyber threats are evolving so quickly that it's important to communicate on a regular basis as the landscape changes."-R10

4.3.4 Theme Three: Challenges of CS Integration in BIM-FM

Theme three investigates the barriers and challenges of integrating cybersecurity within BIM-FM organisations.

This theme entails three sub-themes that each present inhibiting factors of integration at various levels of strategy development, implementation, and performance (execution). Identifying the existing barriers to integration along with the enabling determinants presented in themes I and II, illustrates the steps that can be taken to achieve a successful integration of cybersecurity within BIM-FM. An overview of each sub-theme is described in the following sections. The empirical results showcase the relevance of each sub-theme throughout the analysis.

4.3.4.1 Sub-Theme I: Inhibitors at Strategy development layer

This sub-theme presents the inhibiting factors associated with the integration of cybersecurity in BIM at the strategy development layer. These factors address the existing challenges and shortcomings within the facilities management organisations that impede a successful

management of cybersecurity and jeopardise the achievement of the full benefits of BIM as a result.

Through the interpretation of responses, it was identified that the integration of cybersecurity within BIM strategies was not well managed. Respondents expressed that a lack of a top-down approach in cybersecurity has adversely affected their approach to BIM and hence, most organisations lack cybersecurity considerations within their BIM strategies. Respondents have specifically indicated that if cybersecurity is integrated with a top-down approach, it feeds the feeds down through robust strategies that lead the processes and procedures. Although the importance is acknowledged by the respondents, yet there are concerns regarding a lack of cybersecurity leadership within the facilities management organisations:

"There needs to be that consciousness of the importance of cybersecurity, and it needs to be applied to every task. For people to see it as important as the data itself. There should be a top-down approach because if it starts with the top then it would easily cascade down"-R21

"There is a lack of awareness and the need for training and perhaps there is a lack of a top-down push"-R10

Another inhibiting factor that impedes successful cybersecurity management is the differences in BIM and cybersecurity maturity within facilities management organisations. Organisations have adopted advanced BIM authoring tools and demonstrated high levels of modelling skills but lacked robust data-exchange processes that encompass cybersecurity best practice at their core. Hence the main focus is inclined towards the model rather than the process. As exemplified by the following comments from respondents:

"The traditional BIM guys, for them BIM is the geometric model, but it should be understood much wider, but people can't just get their head around it"-R19

"Well, I would say you have to have strong modelling and data base skills, definitely, you have to sort of have the communication skills as well"-R21

11 of the respondents also expressed dissatisfaction with the standards and guidelines available and the way these have been developed by the professional regulating bodies. They raised concerns regarding the practicality and applicability of the standards and guidelines (e.g.,

PAS1192-5) by stating that they lack examples and case studies that would have assisted the industry with compliance. It was also stated that the lack of industry engagement in the development of guidance documents has resulted complexities within the industry. One respondent stated:

"I think it's that point that the fault is with the industry I think it is the fault of two areas. One is CPNI and the people who wrote part 5 because they didn't make it consumable enough with examples, and this is the fault of UK BIM Alliance for not engaging properly in the educational world…."-R9

Furthermore, respondents pointed to the overly generic statements within the standards and guidelines which allows multiple interpretations. Hence, the organisations compliance with standards and guidelines is dependent on their understanding and competencies in translating and interpreting them for their own use. Considering the multi-stakeholder nature of the BIM-FM projects, every stakeholder will have their own understanding of best practice, causing inconsistencies with processes and procedures and eventually affecting the quality of collaboration. One respondent stated:

"… The problem is they don't tell what should be done so they assume the person who is responsible for the security knows what he is securing … so sharing of information happens in a way that gives access to who needs to know it, that level of intimate knowledge isn't in the industry anywhere at the moment."-R22

The existing cost-driven culture in the facilities management organisations has been identified as one of the key inhibitors of the successful integration of cybersecurity in BIM-FM. Respondents have expressed that not only cybersecurity, but BIM adoption is hugely affected by the cost-driven decision making within FM. This has been confirmed by the following comments of respondents:

"In terms of maturity of infrastructure facilitating BIM projects, these are cost driven, so it is really up to the budget available and the facilities management organisations are usually reluctant to move towards full implementation of cloud-based systems"-R14

"It is always associated with a cost …When we try to explain to them that it's a system for tracking information, it's a system for controlling who gets to see what and when they start to realise that there are benefits to it but there is still a cost that they have to find the money to come."-R6

4.3.4.2 Sub-Theme II: Implementation Inhibitors

This sub-theme presents the barriers and impediments of integrating cybersecurity within BIM implementation in facilities management organizations. The identified inhibitors pertain to the factors that threaten the cybersecurity of processes and procedures within a BIM-enabled project.

Within the interviews, a lack of process formalisation and documentation is reported by 14 respondents. They have indicated that the working processes are hugely dependent on the client requirements and change for every project and every client. As the following respondents state:

"… It depends on the customer requirements if you need a secure environment, because it could come under central government requirements or it could be private sector because they are doing sensitive work that would derive the cybersecurity issues in there."-R20

"…I mean does the FM sector look at the cybersecurity? in my experience no they don't at all! and then does the client specify how the model is going to be used within the FM world? Some do and some don't."-R13

Furthermore, respondents pointed out that the facilities management organisations should develop the information requirements of each task area and believe that this can positively affect the success of cybersecurity management within the BIM projects. Two respondents said:

"A client who is able to define the requirements in terms of the digital information needs and processes, it's absolutely crucial to the success of the project."-R25

"BIM within facilities management is only beneficiary if there is valid data available which can be managed and if the facilities management know which data is required for which task then there can be some sort of use of BIM capabilities …"-R16

Respondents also discussed the inconsistent processes and procedures adopted by various stakeholders involved within BIM-enabled projects. Respondents have specifically pointed out that the diversity of processes and organisational regulations was a key determinant influencing the quality of collaboration within BIM-enabled FM projects. As one of the respondents commented:

"…people tend to simplify them (i.e., process requirements set in guidelines and standards) and every organisation has their own preferences until that has become more homogenised and compatible"-R19

Respondents further elaborated on this issue by stating that the inconsistencies also affected the stakeholder's cybersecurity maturity and hence, not all stakeholders would be able to live up to the cybersecurity management standard suggested by best practice guidelines and standards. It has also been mentioned by the respondents that the size of organisations also contributes to the discrepancies by affecting the capabilities and competency levels. This was supported by the following respondents:

"… I have not seen much of it (cybersecurity measures in BIM-enabled FM) at all except on things that are overtly secure you would imagine they are doing this anyway. I would suggest that you probably find more larger organisations successfully adopting cyber secure BIM"-R8

"So, our team is very small. We are around 35 people within a massive organisation. I would be responsible of taking care of the cybersecurity of data…"-R11

Respondents raised that the successful management of cybersecurity within BIM-FM organisations requires knowledge and skills of both FM and IT related concepts. They further indicated that due to the complexity of the issue of cybersecurity requires effective communication and collaboration between the two teams. One respondent stated that:

"…the problem I see is allocating resources to that, so it's another undertaking that would probably need a little more collaboration between our own security department but at the moment it hasn't happened to the degree that it probably needs to."-R23

The current status of the facilities management industry is more inclined towards a silo approach to cybersecurity management. 16 of the respondents have also demonstrated their organisations over-reliance on IT measures. The statement below exemplifies that view:
"The understanding of the risks at the senior management levels is woefully lacking and they think it's just a job for the IT guys and we might get the occasional spam emails and that's it, but I don't think they realise that a deliberate attack on any technical systems can have existential consequences."-R2

Different views have been expressed on the individual or team responsible for cybersecurity. In the majority of responses, the lack of cybersecurity responsibility was either directly quoted by the respondents or interpreted from their comments. In light of this, the statements which directly raised the concern for the lack of cybersecurity responsibility is presented below. The statement specifies that it is critical to assign cybersecurity responsibilities to a competent body.

"I believe the responsibility is lost within the organisations and specifically with the facilities management, there is extreme lack of process and lack of knowledge in terms of monitoring cybersecurity of data. The responsibility should be with the information manager or the project manager whatever it's called but there should be someone responsible."-R2

Also, the following comments were made by the respondents and interpreted by the researcher. Interpretation of the comments suggest that the lack of knowledge, skills, and awareness as well as a lack of a risk aware culture has resulted an over reliance on IT and technology providers to protect facilities management against cyber security threats:

"This (cybersecurity) is the responsibility of the IT department and not us. you know we're in the same team. We work for the university. IT department and we are all part of the university."-R7

"This I believe is the IT responsibility. I am not involved in the process, so I won't be able to provide any information"-R9

At last, respondents also emphasised that every individual who is involved in a BIM project should be held responsible for the way they use the data and systems. Hence, cybersecurity should be part of all employees' responsibilities. As stated by the following respondent:

"…it's extremely important to take into considerations the user interaction with digital systems and of course every single person involved with a BIM project has a responsibility to behave and perform in a secure manner…."-R1

4.3.4.3 Sub-Theme III: Inhibitors of cybersecure performance in BIM-enabled FM

This sub-theme illustrates findings from the interviews which pertain to the impediments of cybersecure performance within BIM-FM organisations. Amongst the identified impediments, a lack of knowledge and skill was found through thematic analysis of the respondents comments. Respondents raised this as a major shortfall within the facilities management industry. The lack of knowledge of BIM processes, data requirements and best practice guidelines and standards have been stated by the interviewees. The following comments exemplify the abovementioned view:

"…from the majority of government clients that I know out there is that they are telling us that they are using BIM, but they are not they are still using drawings. if the people looking at the document and not even really looking at the document let's say the way you and I understand how they should use it the chances of them even thinking about the security is probably quite remote"-R5

"…the difficulty with this is that the whole BIM and digital security within the space is not business as usual security. So, what often happens is that it gets overlooked. And it either gets in to the "it's all too difficult" box or "we don't understand it" box so we are not going to do it…"-R13

Lack of technical skills in using BIM authoring tools and BIM-enabling infrastructure and networks is found as another barrier to the cybersecure execution of BIM. Respondents have indicated that lack of technical proficiencies amongst the non-technical facilities management employees result in an over-reliance on IT measures and hinders their accountability toward

performing securely. This finding was interpreted from the statement of respondents, some of which are presented below:

".. It's more to do with the IT guys and we just follow what we think it's right. IT just tries to make it simple for us. If anything happens, we just call the IT to help us with it. "-R12
"I am not sure; I wouldn't know in detail but again this isn't my area of expertise it's down to the technical professionals."-R4

19 of the respondents either showcased or directly stated a lack of focus on cybersecurity in BIM-FM. They claimed that cybersecurity was an ad-hoc option, and it is not included in formal project documentations, except when the requirements of the client state that it should be included. Respondents comments follow:

"… Some do include bits of cyber security but the majority not that I have seen much."-R3
"From those very few BIM-enabled FM organisations, there are even fewer organisations who even consider information security and they only do if they are asked to. So, it's not a random practice."-R5

"They don't get involved with security on a day-to-day basis, so it doesn't affect their delivery!"-R22

Furthermore, respondents indicate that cybersecurity is usually deemed as consuming cost, time and human resource and is only considered important in exceptionally sensitive projects. Some respondents further insist that cybersecurity must be embedded in strategies and processes and should be a way of working. They also stated that cybersecurity should be considered in the training and educational programmes. However, they are all in agreement that the facilities management organisations are yet very immature in this regard. Hence, the lack of a security-minded approach to BIM in FM should be addressed. The statements below exemplify this:

"As with any technology, cybersecurity should be considered but I do not think this is a current practice"-R16

"…if you have a high-profile sensitive project then you might find some security considerations, but this is not common practice across the facilities management industry"-R9

A thematic analysis of the responses to the cybersecurity-related questions showed a lack of awareness of risks associated with BIM and digitally enabled FM projects. Although many respondents were aware of the various implications of a cyber-attack in BIM, some lacked insight and awareness of the vulnerabilities concerned. Amongst those who were not aware of the risks, many claimed that as long as the passwords, firewalls and alternative technical security measures are in place, FM should not be held accountable or involved in cybersecurity. In the light of this, respondent 17 comments:

"Security of information…, I don't think that is such an issue! No, I don't think we would have concerns in that direction. I can understand that would be an issue for larger commercial projects but in the public services I don't think it's an issue. In a BIM project, it wouldn't be anything other than the usual checks on IT systems."-R17

Furthermore, other respondents emphasised that a risk assessment which includes cybersecurity risks could help to educate FM about the cyber threats and their impact on the organisation and their assets. They further insisted that the outcome of risk assessments should be passed on to FM at all levels, to ensure a top-down approach as well as a risk-aware culture across all teams within the organisation. The comments of two of the respondents were:

"There should be a security-minded approach in a security risk assessment. To me cybersecurity is just one aspect of information security but within the BIM environment it's the main aspect of information security."-R11

"… We have a total lack of awareness and a total lack of concern about cybersecurity. Until we get to a further point up the stream, if you raise that just about that little benchmark, you will have massive improvement just with that."-R14

4.4 Conclusion

This chapter presented the results of the primary data collection using interviews. The thematic analysis of interview transcripts was described, and themes and sub-themes were presented following a multi-step coding procedure.

The themes illustrated the determinants of a successful implementation of BIM in FM, along with the determinants of successful management of cybersecurity within BIM-FM. The determinants were organised into three sub-themes of strategy, implementation, and performance within the BIM-FM organisation. The analysis of transcripts also highlighted the challenges associated with the integration of cybersecurity in BIM-FM, which were categorised as the third theme. It was identified that the general knowledge and awareness of the cybersecurity considerations within FM is generally limited or restricted by the tasks they are involved in and the problems they face in their day-to-day job. Also, findings demonstrate a considerably limited BIM knowledge in FM, which can lead to immature and inconsistent ways of working. These challenges have a significant effect on different aspects of a BIM in FM, including the cybersecurity of digital data exchanged and archived for various FM tasks. These considerations further led to the identification of more determinants contributing to a cybersecure BIM in FM.

Thus, the next chapter will present a discussion of the findings through synchronising the empirical (chapter 4) and theoretical (chapter 2) findings to enhance and improve the primary-research framework.

Chapter Five: Discussion

5.1 Introduction

This section presents a discussion of the research findings and their contribution to addressing the third and fourth research objectives. The empirical (Chapter 4) and theoretical (Chapter 2) findings are discussed to show the patterns conveyed through the identification of interchangeable characteristics of codes as well as their connections to the primarily identified findings from the secondary data analysis. Section 5.2 presents the discussion of findings at each layer of strategy, implementation, and performance, leading to the refinement of the primary research framework in section 5.3. The chapter is finally concluded in section 5.4.

5.2 Assimilation of findings

The primary data collection explores the factors contributing to a successful management of cybersecurity within BIM-enabled facility management (BIM-FM) organisations by employing a qualitative thematic analysis of interview transcripts. Thematic analysis seeks to explore the understanding of the interview respondents and provide an overview of the concepts of BIM and cybersecurity management in facilities management. The thematic exploration of ideas is based on the extrapolation of three groups of findings:

I. The strategic, implementational, and performance-centric gaps identified from the literature (Chapter 2).

II. FM applicable BIM determinants (Secondary data analysis) (section 2.5.1.2).

III. Determinants of the successful management of cybersecurity within organisations (Secondary data analysis) (section 2.5.2.2).

Following the thematic analysis of the interview data, and for maintaining consistency with the structure of literature-review findings, the cybersecurity integration within the facilities management organisations is investigated for the three layers of strategy, implementation, and performance. Determinants pertaining to each of these layers are discussed in the following sub-sections.

5.2.1 Strategic Integration of Cybersecurity in BIM-FM

Hopkin, (2018) describes strategy as the business goal or target that defines what the organisation aims to achieve. However, Kaplan, (2011) provides a more comprehensive definition, by emphasising the importance of formalising the ways in which organisational aims and objectives can be reached through a structured plan of work, which forms the organisational strategy. To develop a competent strategy, the literature review supports the idea of identifying the determinants that enable the accomplishment of business goals (Caralli and Wilson, 2004). Anderson, (2003) emphasises that the lack of a clear understanding of the sector-specific factors contributing to the successful management of cybersecurity within organisations lead to unproductive strategies being implemented.

This section discusses the main determinants identified for establishing a cybersecure BIM strategy within facilities management. Understanding the underlying determinants of a strategic integration of cybersecurity in BIM and aligning them with organisational BIM-objectives are the main scope of this section. Findings from both the secondary and primary data articulate how information management and the cybersecurity aspect of work tasks are managed within a BIM-FM organisation. The determinants identified were either directly quoted by the respondents or interpreted from their responses to the interview questions. Alternatively, the inhibitors and challenges of cybersecurity integration at the strategy level provided additional insights and offered a more complete picture of the baseline determinants of strategic integration. These determinants are presented in the table 6 below:

Table 6-Strategy Layer Themes and Sub-themes

Theme I: BIM-FM	Theme II: Cyber Security Management	Theme III. Challenges of CS Integration in BIM-FM
Strategic Determinants	Strategic Determinants	***Inhibitors at Strategy development layer***
BIM Leadership (5.2.1.1)	Prioritisation (5.2.1.2)	***Silo Approach to CS in BIM-FM***
BIM strategy development (5.2.1.4)	Value Identification (5.2.1.3)	***Lack of leadership***
Regulations and Standardisation (5.2.1.7)	Organisational Modelling of Information Security Requirements (5.2.1.5)	***Inconsistent BIM & CS Maturity***
	Budget Allocation (5.2.1.7)	***Low Investment***
		Limitations in Standards and Guidelines

5.2.1.1 *BIM Leadership*

Respondents 11 and 12 commented that the facilities management organisations need to take steps towards leading the BIM implementation process (Section 4.3.2.1). Respondents'

comments in section 4.3.2.1 regarding the BIM documentation based on the standards and guidelines, identifying information requirements, budget allocation for improving BIM implementation as well as establishing a collaborative working relationship between the FM and IT departments, illustrate the abilities required to lead BIM in the right direction. In this regard, Sackey *et al.*, (2013) has also stated that BIM leadership pertains to the development of a strategy plan to achieve the purpose of BIM implementation. Therefore, it can be concluded that the BIM leadership determinant encompasses the Purpose of the BIM-implementation determinant which was identified from the literature (section 2.5.1.2.1).

Wong *et al.*, (2000) has also emphasised on the significance of identifying the "purpose" to set the direction for the strategic plans. Hence, leadership is believed to demonstrate the commitment of the management team in stepping towards the organisational goals, such as the successful management of cybersecurity (Selamat and Ibrahim, 2018). Thus, For the integration of cybersecurity in BIM strategies, there needs to be leadership that sets the right visions, missions, and objectives for the development of strategic and implementational plans.

The "RICS BIM for project managers" insight paper (2017) has stated the importance of leadership in translating the purpose of BIM implementation (e.g., visions, missions, objectives) into actionable strategic plans that enable organisation-wide implementation of BIM. As presented in Section 4.3.2.3, respondents also acknowledged the importance of the knowledge and capabilities of senior management teams in the cybersecure leading of BIM, in compliance to the cybersecurity standards, and with respect to the organisational business goals and objectives. The empirical data in section 4.3.3.1 demonstrated that the BIM management team should have cybersecurity high on their priorities list to lead a cybersecure implementation of BIM for all processes and procedures (R1, R9).

5.2.1.2 *Prioritisation*

One of the frequent comments amongst the respondents (e.g., R1, R9 in section 4.3.3.1; R17 in section 4.3.3.3) was that cybersecurity was not the priority of facilities management. It was also described as a matter which is not being considered within the facilities management organizations at all (e.g., R9,16 in section 4.3.4.3). Prioritisation in the context of organisational management refers to the formation of a base for allocating resources for a specific cause (Apostolopoulos *et al.*, 2016). Respondents claimed that prioritising cybersecurity in the development of BIM strategy would stream cybersecurity considerations down to all processes and procedures (Sections 4.3.2.1, 4.3.3.3).

Respondents (e.g., R2 in section 4.3.4.2) stated that the prioritisation of cybersecurity requires an understanding of cybersecurity risks and their impacts at the top-management level and amongst senior decision-makers. Respondents also claimed that identifying the value of integrating cybersecurity encourages the introduction of effective cybersecurity-management plans, however, this is reliant on the evaluation of the value of information and assets and the potential losses in the case of a cyber-attack (section 4.3.1.2 and 4.3.3.2).

Many researchers in the enterprise risk management domain have previously considered prioritisation as a strategic approach to define the organisational risk appetite for the top organisational priorities (Lam, 2017). Studies have indicated that prioritisation should be undertaken by the leaders and the managerial team who are involved in the strategic decision-making. Hence, it is suggested that prioritisation of cybersecurity should be made based on the organisational goals and risk appetite and in compliance with the standards and guidelines (EY, 2017). Therefore, it is concluded that the BIM leadership determinant (section 5.2.1.1) should be accompanied by cybersecurity prioritisation, to enable the integration of cybersecurity in strategic decision-making.

The literature also suggests that the prioritisation should be undertaken as a collaborative task between all departments of an organisation. COSO, (2017), asserts that a siloed approach would lead to a false interpretation of what needs to be prioritised (e.g., the IT department would propose different requirements than the FM team, hence a balanced figure can only be achieved through effective collaboration of both teams).

5.2.1.3 *Value Identification*

Value identification was interpreted from the responses of the respondents as an influential BIM-FM determinant, supporting better strategic decision-making. This result aligns with the Business-enablement determinant that was identified from the literature (section 2.5.2.2.11). Value identification illustrates the impact of certain practices and applications on an organisation. (Iden *et al.*, 2017). Similarly, business enablement takes into account the value of an application or practice on the management of organisational goals and objectives (BSI, 2012).

Many respondents commented that having a risk assessment that includes cybersecurity risks can aid with value identification by identifying potential losses resulting from a malicious cyber intrusion (section 4.3.3.2). Accordingly, value identification assists with the recognition of the ways in which business can maximise value through the uptake or improvement of certain

strategies and practices (Bohnert *et al.*, 2019; Shad *et al.*, 2019; Slagmulder and Devoldere, 2018).

The literature also suggests that the adoption of BIM within FM organisations increases value by facilitating enhanced collaboration and communication, as well as increasing efficiency of working processes (section 2.3.2). Likewise, the risk matrix presented in section 2.4.3 illustrated that a lack of effective cybersecurity management may compromise the values brought by BIM in FM. This can be avoided by the employment of effective cybersecurity risk-management strategies to create value for organisations (Chronopoulos *et al.*, 2017; Gordon *et al.*, 2015). Such values are derived from an improved management of cybersecurity risks, creating a risk-aware culture which leads to risk-aware decision making at board level and eventually, an increased return on investment (Bohnert *et al.*, 2019; COSO, 2017; Farell and Gallagher, 2015). Respondents also claimed that it was difficult to demonstrate the pounds and pence of the value (R3 in section 4.3.3.1). In this regard, the report by (McGill, 2018) points to the challenges and limitations of identifying and measuring such values. As identified in Section 2.5.2.2.11, the value of deploying a cybersecurity management strategy takes into account the effects of cybersecurity risks on the accomplishment of organisational goals and objectives, as well as the business functions and operations. Therefore, it enables a balanced approach towards a cybersecurity implementation of BIM in FM.

5.2.1.4 BIM strategy development

Sections 2.5.1.2.4 discussed the importance of having a competent management plan for the implementation of BIM and highlights the importance of aligning organisational strategy with the BIM implementation plans. Section 2.5.1.2.1 further discussed the importance of having a strategy which transforms the BIM purpose to actionable plans of BIM implementation. This translates into the need for a BIM strategy that pertains to the vision of what an organisation strives to accomplish, through the adoption and implementation of BIM (Kassem et al., 2013).

Many of the interview respondents, (e.g., R12, R24, R9 in Section 4.3.2.1), pointed to the importance of including the development of formal BIM documentation as part of the BIM strategy such as the Employer Information Requirements (EIR) and the Organisational Information Requirements (OIR). Respondents indicated that although cybersecurity is not commonly addressed in such documents, it is critical to include cybersecurity considerations in the BIM documentation (e.g. R9 in section 4.3.3.1). Chunduri et al., (2013) has also emphasised the importance of ensuring process consistency by developing a competent strategy

that is communicated throughout the whole organisation. This entails the development of information requirement documents and establishing the action plans in accordance with the organisational goals (Foss and Michailova, 2009).

Hence, the development of a competent BIM strategy that includes cybersecurity results in cybersecure decision-making throughout all the processes. For this to be achieved, respondents claimed that the competency of the senior management team is critical (e.g., R1 in section 4.3.2.3). A majority of respondents also pointed out the importance of the standards and guidelines in ensuring the development of a cybersecure BIM strategy that will act as a reference for the processes employed at the implementation layer (e.g., R1, R16 in section 4.3.3.1). This was also identified as part of the findings in section 2.5.1.2.7, where compliance with best-practice guidelines and standards was recommended for the development of BIM documentation, as part of a BIM strategy. This concludes that BIM strategy development is supported by both theoretical and empirical findings as a determinant which contributes to the cybersecurity of BIM processes and procedures in FM.

5.2.1.5 Organisational Modelling of Information Security Requirements

The interviews demonstrated that the level of risk tolerance is critical to maintain a balanced approach towards integrating cybersecurity within BIM-FM organisations (e.g., R19, section 4.3.3.2). Respondents argued that excessive lockdown of information jeopardises business objectives and will act as a barrier to the normal operations of a facilities management organisation (e.g., R4, section 4.3.3.1). Respondents also pointed to determinants including value identification and senior management team competencies for managing BIM and cybersecurity oversight amongst the decision makers and claimed that such determinants would assist with identifying organisational information security requirements.

Findings from Section 2.5.2.2.10 have also acknowledged the importance of this determinant as part of the cybersecurity leadership competency. Organisational information requirement modelling may be used as a reference for the implementational procedures (ISACA, 2014; Whitman and Mattord, 2012). Such requirements are based on the organisational visions and goals and need to be established by the senior management team (Barlette and Fomin, 2009). As identified in section 2.5.2.2.10, The senior management team in BIM-FM organisations must be able to define a framework that defines the boundaries of risk tolerance and make strategic decisions aligned with the framework. This will facilitate an integration of cybersecurity within strategic decision-making in the BIM-FM domain. Hence, the BIM

strategy will include cybersecurity elements which will feed through to the implementation plans and processes.

5.2.1.6 Regulations and Standardisation

A number of respondents have commented that compliance to the best-practice documents and guidelines is an effective way of reducing the inconsistencies amongst stakeholders working processes (e.g., R14, section 4.3.3.1), however, some have argued that the diverse capabilities amongst different stakeholders acts as a barrier to compliance with best-practice guidelines and standards (e.g., R6, 4.3.3.1; R9, 4.3.4.1). This supports the theoretical findings in section 2.3.3 where the barriers to compliance with guidelines and standards has been discussed. The comments of the respondents demonstrate a lack of investment towards compliance as a result (e.g., R5, R13, section 4.3.4.3). A lack of compliance with standards and guidelines has a negative impact on the strategic decisions, which may lead to an increase of cybersecurity vulnerabilities in organisations (Berkman *et al.*, 2018). Standards and regulatory documents play a key role in driving investments for cybersecurity management and risk control (Gordon *et al.*, 2016). In this regard, Beautement et al., (2009) claimed that mandatory standards and guidelines are considered as a driving factor for positively influencing budget allocation and investment to enhance organisational cybersecurity capabilities.

Findings identified in sections 2.5 showed limited adherence to the cybersecurity of BIM in facilities management organisations. Efforts were made towards developing BS1192-5 (British Standards Insitution, 2015) which was recently superseded by the ISO19650-5 standard. However, both documents are generalised for use in all phases of a BIM project, without addressing the specific requirements for a BIM-FM organisation. Limitations in guidance for a cybersecure implementation of BIM in FM has resulted in a customised approach to compliance. Some respondents argued that to integrate cybersecurity best-practice guidelines in the BIM strategy, international security standards such as ISO 270001 and BIM standards and guidelines such as the PAS suite, should be combined to provide a comprehensive approach to cybersecurity in BIM (e.g., R3,23, section 5.3.2.3). Considering the variety of standards and guidelines identified in Section 2.5.2.1, this could result in an inconsistent approach towards standardisation amongst the stakeholders. Nonetheless, findings in section 2.5.1.2.7 suggest that an active use of policies, standards and best-practice guidelines can lead to a higher level of maturity within organisations.

Although primarily identified as a contributing determinant in chapter 2, the respondents illustrated the internal and external aspects of compliance. The internal aspects of compliance pertain to the efforts of organisations to facilitate compliance with best-practice guidelines and standards. The comments of the respondents showed an interdependency of compliance with other determinants such as BIM leadership competency, strategy development, budget, knowledge, and awareness (e.g., R15, section 4.3.2.1; R25, R22, section 4.3.2.2). External factors pertain to the regulatory bodies and the efforts made to educate organisations on the use of such standards. Compliance is also associated with other external factors such as penalisation and certification from governing bodies (e.g., R14, section 4.3.3.1; R9, section 4.3.4.1). Although the internal aspects of compliance were taken into consideration prior to the interview (section 2.5.1.2.7), the responses illustrated the external aspect of compliance as well as offering a more detailed view on the internal aspects. Respondents believed that both external and internal factors can significantly contribute to the maturity of an organisation in terms of its compliance. Therefore, the compliance determinant was replaced with regulations and standardisation to address both external and internal factors.

5.2.1.7 Budget Allocation

The lack of sufficient fund allocation for the adoption of BIM at a mature level has been identified as the key inhibitor of cybersecurity within facilities management organisations. A majority of respondents pointed to the cost-driven nature of the facilities management organizations and claimed that the priority was to operate with the least cost (e.g., R14, R6, section 4.3.2.3). Hence, investments in training and educational programmes, and BIM infrastructure and authoring tools, would be undertaken with a focus on cost, rather than quality.

Respondents also claimed that value identification would encourage investment on a secure BIM adoption and implementation, whilst avoiding bias in the budget allocation by identifying the risk appetite and information requirements (e.g., R19, section 4.3.3.3). The comments of respondents further demonstrated a connection between leadership competencies (e.g., knowledge of BIM and awareness of cybersecurity risks) with budget allocation (e.g., R11, section 4.3.3.1).

Sections 2.4.3 and 2.4.4 discuss how the impact of a cybersecurity attack on a BIM-FM organisation compromises the benefits of BIM. This concludes that the cost of implementing BIM would increase, in order to recover from an attack. Accordingly, many respondents

identified the difficulty in quantifying these losses, insisting that not all losses are either quantifiable or predictable (e.g., loss of reputation). Thus, needs to be an understanding of the likely risk impact amongst the senior decision-makers within the facilities management organisation. This supports the findings in section 2.5.2.2.10, where the senior-management team was encouraged allocate sufficient budget towards the cybersecure implementation of BIM in FM. Therefore, the allocation of sufficient funds towards facilitating cybersecurity training for employees and fulfilling the cybersecurity requirements has found to contribute to an improved cybersecurity within BIM-enabled FM.

5.2.2 Implementational Integration of Cybersecurity in BIM-FM

This section discusses the key determinants contributing to cybersecurity in BIM implementation within the facilities management organisations. As (Hopkin, 2014) states, the success of integrating a concept such as cybersecurity within the strategic layer is dependent on the implementation. It is hence considered that implementation is a prescription for achieving strategic objectives within the deliverables of performance (Andronache, 2019). Mankins and Steele, (2005) define implementation as the connecting link between the strategy and performance. Furthermore, implementational factors are identified as determinants that are built upon both the structures in place and the managerial competencies (Thompson *et al.*, 2018).

The empirical findings in Sections 4.3.2.2, 4.3.3.2 and 4.3.4.2 present the implementational determinants that contribute to a cybersecure implementation of BIM in FM. These determinants entail activities, programmes, systems, interactions and monitoring that provide the means of connecting strategies with performance (Mankins and Steele, 2005)

To explore the integration of cybersecurity within the implementation layer, the review of literature illustrated a number of determinants pertaining to, both the successful implementation of BIM in FM, and the integration of cybersecurity within an organisation. Hence, empirical data collected during the interviews provided an in-depth oversight of the applicable determinants in a BIM-enabled facilities management by the exploration of integration challenges and inhibitors, as well as extracting integration enablers from the comments of the interview respondents. The determinants contributing to the integration of cybersecurity at the implementation layer are listed in the table below:

Table 7-Implementation Layer Themes and Sub-themes

Theme I: BIM-FM	Theme II: Cyber Security Management	Theme III. Challenges of CS Integration in BIM-FM
Implementation Determinants	Implementation Determinants	**Inhibitors at Implementation layer**
Defined BIM-FM Processes (5.2.2.5)	Cybersecurity Design (5.2.2.2)	**Lack of Formalised Processes**
BIM Infrastructure Maturity (5.2.2.3)	Risk Management Plans (5.2.2.1)	**Budget Limitation**
Defined Information Requirements (5.2.2.6)	Defined Security Processes (5.2.2.5)	**Lack of IT & FM Liaison**
Monitor & Audit Processes (5.2.2.7)	Arrangement of Cybersecurity Duties (5.2.2.9)	**Lack of CS Responsibility in FM**
Pre-tender Competency Evaluation (5.2.2.8)		**Inconsistency of Process Across Industry**

5.2.2.1 Risk Management Plans

A cybersecurity risk management plan was identified as a key determinant by many researchers in the technology and system-security domains (section 2.5.2.2.2). Risk management plans are developed to evaluate and mitigate risk following the identification of their nature and extent, in order to ensure the accomplishment of the organisational objectives (Joint Task Force, 2018). In this regard, the interview respondents illustrated the importance of identifying cybersecurity risk in BIM-FM, however, a majority of them were in consensus about the lack of cyber-risk management within their organisations (e.g., R25, section 4.3.3.2). The underlying cause of this shortfall was claimed to be a lack of financial and human resources to undertake the risk assessment (e.g., R23, section 4.3.3.2). Many respondents also pointed to a lack of risk oversight at board level, resulting in cybersecurity being overlooked amongst other risks. Empirical findings show that facilities management organisations commonly focus on the financial and health & safety risks, whilst cyber risks are not taken into consideration (e.g., R17, section 4.3.3.2). Section 2.5.2.2.2 further illustrates that risk management requires an established strategic approach that incorporates resources, technological facilities, and knowledge for the implementation of organisational risk management. Hence, for facilities management to successfully integrate cybersecurity within their risk-management plans, a strategic approach is required to support the facilitation of the training, budget and human resources required for cybersecurity risk management.

5.2.2.2 Cybersecurity system design

Theoretical findings in section 2.5.2.2.1 have recommended that having a cybersecurity system in place to protect the BIM infrastructure would benefit the BIM-FM organisations, providing it is effectively managed and they are designed, managed, and maintained in accordance with the requirements and regulations. The thematic analysis of interviews also showed the significance of cybersecurity system design for the BIM-FM organisations. A majority of respondents claimed that the CDEs and digital tools and systems facilitating BIM projects, required an information security system that is designed to monitor and manage security of data within the digital working environments (e.g., R7, R1, section 4.3.2.2). They also emphasised the need for a collaborative approach between the IT and FM departments to develop and manage the cybersecurity systems (e.g., R23, R21, section 4.3.3.2).

Although a number of respondents criticised the over-reliance of facilities management on IT solutions and disagreed with the isolated approach, other respondents claimed that cybersecurity is not the responsibility of facilities management (e.g., R24, R2, section 4.3.3.2). The latter group further demonstrated a lack of cybersecurity related knowledge and skills as well as a lack of awareness of risks, leading to an over-reliance on IT teams (e.g., R7, R9, section 4.3.4.2). Hence, it is important to have an effective cybersecurity system which is subject to continuous monitoring and improvement through the coordination, collaboration, and effective communication of technical and non-technical teams to obtain BIM-infrastructure maturity

Findings from the interviews illustrated the importance of BIM authoring tools, digital-information sharing platforms and networking systems, in the cybersecurity management of BIM-FM projects (e.g., R17, section 4.3.1.1). Accordingly, the BIM infrastructure maturity was identified in section 2.5.1.2.2, where “infrastructure” pertains to the software, hardware and networking systems used for facilitating access, archiving, and exchange of data within a BIM project.

The empirical data collected from respondents (e.g., R19, section 4.3.4.2) shows inconsistent BIM infrastructure maturity amongst organisations, which resulted in disparities between their strategies, processes, and characteristics (e.g., size of the organisation, budget, etc). This confirms the findings in section 2.5.1.2, where the compatibility of technological advancements and strategic maturity is emphasised by Succar’s BIM maturity model (Succar, 2010, 2015). Hence, considerations for implementation that required BIM infrastructure should include

foundational strategies that can support the uptake of advanced BIM technologies. The successful implementation of BIM depends largely on aspects of technology and social interdependencies within a BIM-enabled organisation (Linderoth, 2010).

Theoretical findings also suggest the development of a process plan for the selection, use and management of BIM infrastructure (section 2.5.1.2.2). Succar, (2015) proposes the development of an implementation plan that includes continuous evaluation and modification of the existing processes around the BIM infrastructure and insists on deploying structured measures for the management and maintenance of hardware, software, and networking systems. Empirical data showed that the aforementioned tasks are commonly rolled out to the IT and technical professionals, however, it is vital for the facilities management teams to incorporate their knowledge in the development of the BIM infrastructure management and maintenance plan (sections 4.3.2.2, 4.3.3.2). Such an approach allows for the integration of technical knowledge for cybersecurity with the facilities management knowledge of information requirements, data exchange processes and operational procedures, and hence, facilitates a cybersecure approach for enhancing the maturity of BIM infrastructure.

5.2.2.3 Defined BIM-FM Processes

The comments of the interview respondents demonstrated that FM processes depend on the client requirements, project requirements and stakeholder procedures. These overdependencies are known to compromise compliance in favour of implementing stakeholder-specific preferences in defining working processes (e.g., R13, section 4.3.3.2). Theoretical findings in Section 2.5.1.2.3 emphasise the establishment of defined organisational processes to ensure transparency of working procedures. These are needed to provide an overview of the organisational capabilities and the areas in need of optimisation and improvement. Establishing well-defined and well-managed processes and procedures is identified to improve on the information security management capabilities within an organisation (Radl and Kaiser, 2019; SEI, 2010). As Empirical findings in section 4.3.2.2 suggests (e.g., R25), developing formal process plans and the development of structured procedures, empower the implementation of strategies and the achievement of organisational goals. A cybersecure approach to BIM-FM would have cybersecurity at its core, hence, cybersecurity should also be incorporated within the processes and procedures to allow a cybersecure implementation of BIM within FM.

5.2.2.4 Defined security practices

Interviews have shown that formal documentation of processes affects the accomplishment of strategic goals (e.g., R25, section 4.3.2.2). The respondents further elaborated that a standardised approach to the development and documentation of security processes and procedures would improve the cybersecurity status of the stakeholders of a BIM-enabled project (e.g., R6, section 4.3.3.2). Findings from the literature also emphasise the need for defined security management processes and procedures along with a well-designed information security system (section 2.5.2.2.6). Both empirical and theoretical findings highlighted the importance of standardisation of cybersecurity processes and the need to communicate them to all members of an organisation to enable a coordinated integration of cybersecurity within all operations.

5.2.2.5 Defined BIM-FM task information-requirements

The need for a competent BIM implementation plan was initially identified in Chapter 4. This determinant identified the need for a number of requirements to be met for the successful development of a competent BIM implementation plan (section 2.5.1.2.1). As identified within PAS1192-2, the Employer Information Requirements (EIR) and Asset Information Requirements (AIR) which feed into the BIM execution plan (BEP) are fundamental principles of BIM level two and are essential to the development of a competent BIM implementation plan (Ashworth, Tucker and Druhmann, 2016). Thus, the "defined task information requirement" determinant is as part of the development of "a competent BIM implementation" plan which was primarily identified in chapter 2. However, because of the emphasis on criticality by the respondents, it was later decided for it to be added as a key determinant. Interviewees have claimed that the identification of task information requirements enabled easier implementation of access permits within a collaborative working environment (e.g., R14, section 4.3.2.2). Furthermore, participants commented further on PAS suite suggestions and instructions, with regard to structuring information within the BIM model. Identifying task information requirements results in better structuring and organisation of information and provides clear insights for better monitoring and control of information sharing protocol (e.g.R20, section 4.3.2.3). Thus, it can be concluded that the identification of information requirements for each FM task would lead to an improved management of cybersecurity in BIM-FM.

5.2.2.6 Monitor and Audit Processes

The ‘monitor and audit processes’ determinant was initially identified as quality control plans in Section 2.5.1.2.8. However, theoretical findings illustrated that the sole focus of the existing studies and models was on the evaluation and validation of BIM models through computerised platforms. Data collected through interviews illustrated the importance of the evaluation and validation of processes and performance to improve cybersecurity within a BIM-FM organisation (e.g., R24, R10, section 4.3.2.2). As part of the quality management processes, ISO 9000 specifies the importance of performance evaluation against benchmarks as well as incorporating performance-improvement plans into the implementation plan. Succar et al., (2013) also recognised that monitoring the process enables informative decision-making on the course of future improvements. Therefore, the “quality control plans” in the primary research framework was changed to ‘monitor and audit processes’, to account for process monitoring and compliance audits, along with BIM quality-check plans.

5.2.2.7 Pre-tender BIM Competency

Inconsistency of processes amongst the stakeholders was identified through the thematic analysis of interviews. Respondents have shared experiences of collaborating with lower-maturity stakeholders in terms of the adoption and use of BIM authoring tools and CDEs, as well as their capabilities in managing and monitoring information sharing processes and procedures (e.g., R4, section 4.3.2.2). Many participants have suggested certification as a way of demonstrating organisational capabilities and competencies. Compliance to the best-practice guidelines and standards have been deemed as a way of encouraging the enhancement and improvement of processes to fulfil the requirements of compliance (e.g., R23, section 4.3.2.2). Participants have also commented that vetting procedures are important to ensure the quality of collaboration. Hence, integration of cybersecurity and the assessment of the cybersecurity maturity of stakeholders and suppliers is important for ensuring a cybersecure delivery of a BIM project (e.g., R13, section 4.3.3.1). Findings from the literature have also recognised the fragmented nature of the construction industry that has entailed inter-organisational culture clashes and inconsistencies in the standardisation of procedures and formal documentation (section 2.3.3). Discrepancies amongst stakeholders involved in a BIM-FM project can range from the organisational characteristics such as size, location and goals to performance, skills and technological capabilities (Cox *et al.,* 2016). This may negatively impact the quality of service/product, Value for Money (VfM) and the overall quality of collaboration and in particular, information exchange processes and procedures (Adegbesan and Higgins, 2011).

Hence, findings from the interviews and the supporting statements from the literature both stand by the significance of pre-tender assessment of the competencies of stakeholders.

5.2.2.8 Arrangement of cybersecurity duties

Despite the uncertainties regarding cybersecurity responsibilities and duties demonstrated by the interviewees, the over-reliance on IT teams and technology providers to ensure and manage cybersecurity was discussed by the majority of respondents (e.g., R2, section 4.3.4.2). The available standards and guidelines within the facilities management and BIM domains recommend the appointment of a built-asset security manager (British Standards Insitution, 2015). However, the cybersecurity responsibilities associated with every role within facilities management is overlooked. A number of respondents suggested that the strategic integration of cybersecurity was reliant on the performance of employees. It was also suggested that every user is responsible and accountable of their interactions with the digital systems and tools (e.g., R1, section 4.3.4.2). Thus, cybersecurity responsibility should be included within every job description.

Although arrangement of BIM-related duties and responsibilities (section 2.5.1.2.5) was identified as contributing towards improved information management, no particular indication of cybersecurity-related duties was found within the existing literature. As proposed by Glantz (2016), organisations must assign and document the accountability of employees for the cybersecurity of information. Theoretical findings further elaborate on the need for a cybersecurity risk-aware culture both at the top decision-making management board level and at the implementation and execution levels (sections 2.5.2.2.8, 2.5.2.2.10). The empirical data also suggests that assignment of cybersecurity roles and duties to competent professionals within the facilities management organisations requires a competent management team to ensure the suitability of the duty assignment (e.g., R1, section 4.3.2.3).

5.2.3 Integration of cybersecurity in BIM-FM Performance

Determinants related to people (employees) of organisations have been discussed amongst both academia (published studies, peer review papers) and professional bodies (standards and guidelines). As emphasised by BSI (2010), it is important to align people competencies with strategic and implementational goals. The empirical findings demonstrate the importance of employee-competencies in handling digital information. A number of participants identified that the cybersecurity responsibility should be included in every job description and should be assigned to every employee who is involved in a BIM-enabled project. It is believed that having

accountability for performing in a responsible and cybersecure manner requires education and training as well as a risk-aware culture which should be established by the senior-management board (sections 4.3.2.3, 4.3.3.3). Da Veiga and Eloff, (2010) further insist on the importance of a security-minded culture as a basis for collaboration and teamwork within organisations and across the industry. However, the empirical data showed a lack of knowledge and skills as well as a risk-aware culture at either the top or bottom management layers of some BIM-FM organisations.

Findings from the literature demonstrated the significant role of the capabilities of people in maintaining the cybersecurity of technology-enabled organisations (section 2.4). In this regard, the social aspect of cybersecurity integration is discussed by the literature. For instance, Braumann, (2018) points to communication, training and education, culture and awareness as the influential factors affecting the cybersecurity of an organisation. Hence, this section will further discuss the determinants that contribute to cybersecure performance within BIM-FM organisations (Table 8).

Table 8-Performance Layer Themes and Sub-themes

Performance Determinants	Sub-theme: Performance Determinants	Sub-theme: Inhibitors at performance layer
Performance Determinants	Performance Determinants	**Inhibitors at performance layer**
BIM senior management team competency (5.2.3.1)	Cybersecurity oversight at board level (5.2.3.2)	**Lack of employee education and awareness**
BIM Knowledge and Skills (5.2.3.3)	CS knowledge & kills (5.2.3.5)	**Lack of security-minded approach to BIM in FM**
	Risk aware culture (5.2.3.4)	**Lack of cs knowledge at BIM management board**
		Lack of risk awareness across FM

5.2.3.1 BIM senior management team competency

The empirical data showed that the adoption and implementation of BIM within the facilities management organizations requires a top-down approach. The quality and effectiveness of this approach is down to the competencies of both the senior-management team and operational teams (e.g., R11, section 4.3.3.2). Respondents argued that assigning roles and responsibilities to qualified teams and individuals requires competency at the top levels of management to develop the right criteria for the selection of human resources (e.g., R1, R14, 4.3.2.3). In this

regard, (Dakhil, 2017)) discusses the extent to which the management provides financial and human resources, legal support and change management, and addresses the impacts of those on the maturity of BIM-enabled organisations. Amongst studies that address the performance-centric measures of BIM, a number of researchers have considered administrational and managerial competencies along with determinants such as education, awareness and culture (Architectural, 2015; Van Berlo et al., 2012). Theoretical findings in Section 2.5.1.2.6, point to the BIM knowledge and skills required to lead and manage BIM effectively. Henceforth, reducing cybersecurity vulnerabilities by minimising the challenges associated with an immature implementation of BIM in FM (Section 2.4.3).

5.2.3.2 Cybersecurity oversight at board level

The interview responses highlighted the performance-centric competencies at the top managerial levels or the board of decision makers. They emphasised that knowledge and awareness of cybersecurity risks at board level, leads to cybersecure decision-making that contributes to the development of strategies that have cybersecurity at their core (e.g., R21, section 4.3.3.3). Many studies have previously identified the role of the board of an organisation in the successful streaming of strategies to all processes and procedures (Cabinet Office, 2012). Theoretical findings in sections 2.5.2.2.10 and 2.4.2.2.8 also acknowledge that the board of managers and directors are responsible for ensuring cybersecurity is integrated throughout the organisation and in line with the overall objectives and goals. To ensure the management team is capable of leading cybersecure ways of working, empirical findings have recommended education, training, and upskilling programmes for the management team and those involved in major decision-making in an organisation (e.g., R10, 4.3.4.1 and R2, 4.3.4.2). According to the findings, it is concluded that cybersecurity oversight refers to establishing management strategies and control measures, to enable the leading of cybersecurity from the top layer of management. Hence, facilitating a top-down approach to the integration of cybersecurity within BIM-FM.

5.2.3.3 BIM Knowledge and Skills

Theoretical findings in section 2.5.1.2.6 showed that BIM knowledge and skills contribute to the fulfilment of other BIM determinants, leading to a more mature implementation of BIM in FM. In this regards, empirical findings also proposed that BIM education, training and upskilling programmes are vital to the integration of cybersecurity in BIM-FM. BIM knowledge and skills amongst the FM organisations was affirmed by most respondents and

was emphasised as a prerequisite for both cybersecurity and BIM determinants (e.g., R5, R13, section 4.3.4.3). For instance, the undertaking of risk management, cybersecurity-system design and BIM infrastructure maturity all require knowledge of BIM tasks and working processes, BIM-information requirements, and the structuring of information in a BIM model. A comprehensive knowledge of BIM entails knowledge of BIM standards and best-practice guidelines and better realisation of the information-management aspects of BIM, which leads to better cybersecurity management of information (Arayici and Aouad, 2011). Therefore, the integration of cybersecurity within BIM-FM is hugely dependent on this determinant and can be facilitated by the collaboration of IT & FM teams. This enables the incorporation of both BIM knowledge from the FM professionals, and cybersecurity and technical knowledge from the IT/security team. Ashworth et al., (2016) emphasises that BIM-enabled organisations need to identify role-specific training and educational programmes to upskill employees BIM knowledge and skills. The fulfilment of BIM roles and responsibilities for strategy and implementation requires knowledge, skills, and experience by people at the top and also those down the line of project implementation and execution. The BIM knowledge and skills at the top level is incorporated with managerial knowledge and skills and hence named as the 'BIM senior-management team competency', which was identified as a determinant in section 5.2.3.1.

5.2.3.4 Risk aware culture

Interview responses demonstrated that for the facilities management industry to fully capture the benefits associated with the adoption of BIM, a transformational shift to the new ways of working is inevitable. Respondents pointed to a culture change that is required to accommodate cybersecure behaviour directed by an awareness of cyber risks, to the BIM-enabled projects within FM (e.g., R19, section 4.3.3.3). Theoretical findings have acknowledged that a risk-aware culture entails knowledge and awareness of cybersecurity risks and their implication to the organisation and its assets, as well as the effective communication skills within an organisation (Section 2.5.2.2.9). In this regard, responses to interview questions demonstrated a lack of communication, symptomatic of a lack of formalised processes for communicating decisions or rules relating to the processes, and procedures, that must be complied with by employees. In particular, respondents argued that if a cybersecurity-risk assessment is undertaken, the results should be effectively communicated to those involved (e.g., R10, R21, section 4.3.3.3).

Both empirical and theoretical findings have acknowledged the importance of a risk-aware culture in the integration of cybersecurity within an organisation. A risk-aware culture which can be established by developing knowledge, skills, and awareness along with the implementation of formal communication procedures.

5.2.3.5 Cybersecurity knowledge and skills

This determinant refers to the cybersecurity skills required for cybersecure performance of everyday job tasks. According to the interview responses, cybersecurity knowledge and skills are a key barrier towards cybersecure implementation of BIM. There is a consensus among the respondents regarding the lack of cybersecurity-related knowledge and skills in facilities management organisations. However, the disagreement was whether knowledge and skills in the cybersecurity domain is necessary for the facilities management employees (e.g., R5,13, section 4.3.4.3). Some of the responses demonstrated that a lack of knowledge in this regard, led to an isolated approach to cybersecurity and resulted in an over-reliance on IT teams (e.g., R22, section 4.3.3.2). Also, many respondents believed that such knowledge was not required for the FM employees, as it was not included in the job descriptions. Therefore, it is acknowledged that organisations need to be transparent about the accountability and responsibility of employees regarding the cybersecurity of information that they are handling as part of their job. A number of respondents argued that the organisations are as cybersecure as their weakest link. Hence, employees must be competent in interacting with BIM platforms and BIM authoring tools and understand the cybersecurity implications to an extent which allows them to perform better whilst protecting information (e.g., R19, section 4.3.3.2).

5.3 Framework Development

This section presents an amalgamation of the findings from the thematic review of the literature, along with the empirical data collected through semi-structured interviews. The empirical findings are incorporated into the primary research framework developed in chapter 2. Respectively, the primary research framework is improved and enhanced with reference to the empirical findings.

This framework is developed to address the third and fourth research objectives, by presenting a synergy of three constructs of evidence:

i. Literature review (section 2.3.3)

ii. Qualitative analysis of secondary data findings pertaining to the identification of BIM-FM and cybersecurity management determinants- Primary research framework (section 2.5)

iii. Thematic analysis of interviews, being the primary data collection for exploring the primary-research framework determinants and the interconnections and existing arguments around the integration of cybersecurity within BIM-FM (section 4.3)

The development of the framework was to achieve the research aim, by developing a framework that supports the incorporation of cybersecurity considerations within BIM-FM organisations. Whilst the theoretical findings facilitated the development of the primary framework, the empirical results deepened and enhanced views on the determinants and their connections, built upon the practical views from the interview respondents. Hence, the third construct offers insight and evidence of the enablers and inhibitors of cybersecurity within BIM-FM, from which the primary research framework was enhanced and improved.

The empirical results demonstrated the enablers and inhibitors of cybersecurity integration at three layers of strategy, implementation, and performance within a BIM-FM organisation. These determinants were identified to address the third research objective and further call on the third research objective by interpreting the interdependencies.

5.3.1 Strategy layer

Evidence illustrated that the successful integration of cybersecurity within the strategy layer required BIM leadership, prioritisation, BIM strategy development, value identification, regulation and standardisation, organisational modelling of information security requirements and budget allocation (section 5.2.1). These determinants were in line with the determinants proposed by the primary framework. However, the empirical findings expanded on the scope of each determinant to include cybersecurity considerations. To exemplify, the primary framework included the purpose of the BIM implementation as a determinant which pertained to the goals, visions, and objectives of BIM. The empirical results demonstrated that it is important to take into consideration BIM leadership that encompasses the responsibility of setting the goals, visions, and objectives instead of limiting it to a single element of purpose. As findings emphasise, BIM leadership includes the identification of purpose as well as leading the organisation towards the achievement of goals in a cybersecure way. Additional changes to the primary framework included the cyber-security leadership which pertained to the cybersecurity oversight at board level and the modelling of organisational information security

requirements. The empirical data further acknowledged these elements as key determinants which belonged to different layers. Hence, cybersecurity oversight at board level was identified as a performance-centric determinant whilst the organisational modelling of information-security requirements was sourced back to the strategic cybersecurity determinants. The empirical results further proposed value identification as a determinant with a similar meaning to the business-enablement determinant of the primary framework, which denotes the value provided by cybersecurity controls in the strategic management of business goals and objectives. As the 'value identification' was frequently addressed, the phrase replaced 'business enablement' to ensure an easier understanding for FM professionals. Empirical results also demonstrated additional determinants such as 'financial resources' which were added to the framework to improve on its inclusiveness.

5.3.2 Performance layer

The empirical results in section 5.2.2 demonstrated that the strategic determinants were dependent on the competencies of the BIM senior-management team and those in the top decision-making chairs who were responsible for developing strategies which complied with organisational goals and objectives. Findings also illustrated the significance of cybersecurity oversight, by top management capable of streaming cybersecurity down the line of implementation and ensuring cybersecurity is incorporated and considered in every process and procedure.

It was further illustrated that successful implementation of strategies was impossible without the competencies of all other employees. Other than the competency of the BIM management-team and cybersecurity oversight at board level, other performance-centric determinants were also identified. Results pointed out to BIM knowledge and skills, cybersecurity knowledge and skills and a risk-aware culture as key determinants affecting the implementation of strategies. The primary framework included BIM knowledge and skills, however, a cybersecurity determinant labelled as 'the competency of security team', was initially identified, which pertained to the importance of cybersecurity knowledge. The empirical data demonstrated that for the integration of cybersecurity, all business functions must have cybersecurity knowledge and skills, to varying extents, depending on their roles. Henceforth, cybersecurity knowledge and skills were replaced with the security team competency to address the cybersecurity knowledge amongst all business functions, including the security team. If cybersecurity knowledge is sourced from the IT or security specialists, effective communication and

collaboration is also required within the FM and IT specialists to facilitate the incorporation of both BIM-FM and cybersecurity knowledge in the implementation of BIM. This will improve on the employee awareness of cybersecurity considerations and encourage cyber risk-aware decision making at the implementation layer. Hence, a 'risk aware culture' determinant was added to the framework as an additional determinant.

The enhancement and improvement of knowledge, skills and awareness was found to be interdependent with the frequency and quality of training and educational programmes. Hence, it was concluded that the management competencies and cybersecurity oversight will feed into the development of a cybersecurity-minded strategy, that will result in the facilitation of training and education programmes which have cybersecurity at their core. The separation of performance determinants into two distinct levels (i.e., top-level and bottom-level) was decided following the aforementioned reasoning. Hence, the primary framework was amended in line with the empirical findings.

5.3.3 Implementation layer

Theoretical and empirical evidence have also identified the determinants contributing to an improved cybersecurity implementation within BIM-FM. These determinants include defined BIM-FM processes, security requirements engineering, BIM infrastructure maturity, cybersecurity system design, defined information requirements, risk management plans, monitor & audit processes, defined security processes and pre-tender competency evaluation. Where the pre-tender competency evaluation of stakeholders was a new addition to the primary framework, The primary framework also included a 'quality-check' determinant which was later changed to a 'monitor & audit processes' determinant to better express that the check refers to a process and compliance check rather than a sole focus on the quality of project deliverables. Furthermore, empirical results insisted on the 'monitoring and audit processes' determinant which the 'quality check' determinant failed to express.

Research findings emphasised the importance of the continuous improvement of strategies and processes, to achieve improved performance. It was argued that the implementation of a security-minded BIM should be followed by auditing, monitoring and quality checks that are communicated to the top-management team to moderate, amend and improve strategies leading to an overall improvement of processes and procedures. That will further allow for the identification of the weaknesses and deficits which need improvement which could be achieved by training and education, investment in infrastructure or assignment of human resources.

5.3.4 Enhancing the scope of BIM maturity

As discussed in section 2.3.2, a mature implementation of BIM is associated with benefits such as the enhancement of productivity or efficient use of organisational resources. Similarly, challenges associated with the implementation of BIM in FM in section 2.3.3 illustrate the inter-relationships between the organisational weaknesses and their effects on achieving a mature implementation of BIM. This includes the cybersecurity management aspect, which needs to be improved for enabling a mature implementation of BIM, and achieving the full potential of BIM in FM.

The integration of cybersecurity with BIM determinants that are provided by the maturity models, will expand the scope of BIM maturity to incorporate mature cybersecurity-management processes. To exemplify this, the existing maturity models have referred to the considerations of BIM leadership (section 2.6.1.3). However, no indication of cybersecurity considerations was found within the current resources. The integration of cybersecurity with BIM leadership means prioritisation of cybersecurity objectives, with respect to the BIM objectives initially set out by the BIM leadership (section 5.2.1.1). Therefore, BIM leadership should enhance its scope to encompass cybersecurity considerations, which would then contribute to the fulfilment of other determinants, by feeding cybersecurity into all processes and procedures.

Another example is the BIM knowledge and skills (section 2.6.1.3.6), already established within existing maturity models. However, the scope of this determinant defined by various maturity models does not encompass cybersecurity considerations. When coupled with cybersecurity knowledge and skills (section 5.2.3.5) and backed by a risk-aware culture for cyber-security (section 5.2.3.4), the scope of the determinant includes the integration of cybersecurity. This does not mean that all employees should have an identical level of BIM and cybersecurity knowledge but what is necessary to perform their role safely and effectively. The integration of cybersecurity with BIM knowledge and skills may be achieved by the synchronisation of knowledge from two different employees/teams within a BIM-enabled facilities management (e.g., IT and FM teams), however, decisions should be made based on information gathered from both BIM and cybersecurity perspectives.

The existing maturity models provide a comprehensive overview of a mature implementation of BIM, with a sole focus on BIM considerations. However, they do not encompass

cybersecurity considerations holistically. The discussion of findings showed new horizons for the existing BIM maturity models, to encompass cybersecurity considerations within the scope of BIM maturity. The integration of cybersecurity determinants with BIM determinants would enable organisations to seek BIM maturity that incorporates cybersecurity. Hence, cybersecurity management will not be segregated from BIM management within the facilities management organisations. The integration of cybersecurity determinants with BIM determinants at three layers of strategy, implementation and performance is only possible by looking at the inter-relationships between various BIM and cybersecurity determinants. In many instances, enhancing the scope of a BIM or cybersecurity determinant would enable the achievement of both cybersecurity and BIM-FM objectives. However, this is dependent on various organisational factors, including the structure, hierarchy of responsibilities, current BIM, and cybersecurity stance, which should be considered by each organisation.

5.3.5 BIM-FM Cybersecurity Considerations

As demonstrated by the cybersecurity risk matrix in section 2.5.2, a breach of the cybersecurity triad results in the compromise of the BIM benefits in FM. Section 2.4.1 and 2.4.2 presented the various threats, that may exploit vulnerabilities in process, technology, and employee performance. Considering the empirical findings, current BIM-FM organisations are not concerned with cybersecurity considerations, and lack the capabilities required for a cybersecure implementation of BIM. Therefore, for improving on the cybersecurity of BIM-FM organisations, a structured approach towards the integration of cybersecurity in strategy, implementation and performance layers of the organisation is required.

The ISO19650-5 which superseded PAS1192-5 in 2020, provides an overview of the cybersecurity considerations within the adoption of BIM. Both documents provide a cross-sectional approach to cybersecurity, where the variety of tasks, level of details required (level of information need) and cybersecurity responsibility of the employees within a specific phase of a BIM project are not addressed. Furthermore, guidance is provided in a generic form to enable cybersecurity to be applied in all organisations (e.g., regardless of size, sector, or role-hierarchy). However, it does not account for the poor capabilities of the FM organisations to effectively interpret the compliance requirements and understand where improvement is required. As identified by the empirical findings, there is a lack of readiness in the current state of the BIM-FM organisations for full compliance with the existing standards. Therefore,

organisations should be guided towards improving their capabilities in fulfilling the requirements, set out in the available standards.

Compliance with such standards and guidelines is found as a key determinant of a cybersecure BIM in FM (section 5.2.1.6). However, empirical findings illustrated that compliance requires the fulfilment of other determinants, to meet the requirements set out by the standards. For instance, Sections 5.2.3.1 and 5.2.3.2 discussed cybersecurity oversight coupled with a competent BIM management team is required for cybersecurity to be considered at the top level of a BIM-FM organisation. Therefore, it can be concluded that these two determinants drive compliance with standards and best-practice guidelines, by facilitating the necessary cybersecurity systems, BIM infrastructure, processes, and resources. Therefore, this research proposes a longitudinal approach to a seamless integration of cybersecurity within strategies, implementation, and performance layers of a BIM-FM organisation.

5.3.6 BIMCS-FM Framework

The primary research framework was built upon the extraction of determinants from Succar (Succar, 2009, 2015) and CIC BIM maturity model (Construction Industry Council, 2013), and the cybersecurity best practice guidelines and standards. The determinants extracted from the BIM maturity models were related to the challenges of BIM in FM, identified from the review of literature (Chapter 2). These challenges were found to act as cybersecurity vulnerabilities in BIM-enabled facilities management, which accentuates the need for a focus on cybersecurity management in BIM-FM. As the BIM maturity models have limited indication to the people and process aspects of cybersecurity, best practice guidelines and standards in the cybersecurity domain were used as a source to extract the cybersecurity determinants applicable to BIM-FM organisations. The integration of cybersecurity and BIM determinants was the foundation of the primary research framework, where the structure proposed a unified management of cybersecurity and BIM in BIM-FM. As the primary framework (section 2.6) was based on the theoretical findings from the secondary data analysis, empirical data was used to enhance and refine the framework, through an in-depth exploration of the concepts of BIM and cybersecurity, and investigation of the applicability of the primary research framework determinants in practice. The assimilation of the empirical findings with the theoretical findings (i.e., primary research framework), contributed to the enhancement and refinement of the research framework through adding the perspective of practitioners and the recognition of the

interconnections between the strategic, implementation and performance layers.

The framework that was developed as a result, proposes a structured representation of the determinants that lead to a cybersecure BIM-FM organisation. Whilst it does not provide the solution, it presents an intellectual construct that directs the facilities management organisations in the development of process models, based on the concepts and connections provided by the BIMCS-FM framework.

Figure 14 presents the modified version of the framework which presents the additional determinants, streamlining and connections which have reformed the framework and transformed it into a cyclical framework.

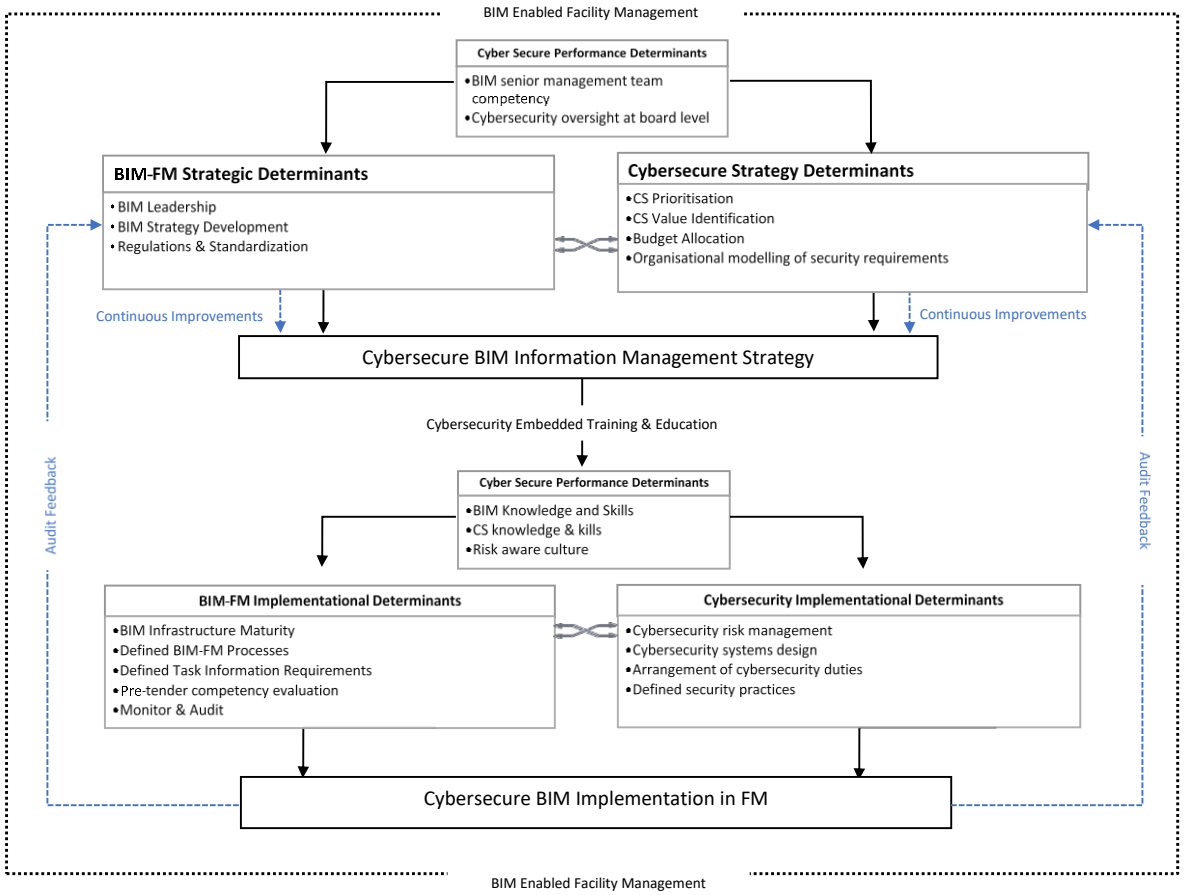


Figure 14-BIMCS-FM Research Framework

The revision of the framework is consistent with the findings from the empirical results, which emphasise the importance of recognising the origin of the domain of the determinant. BIM and cybersecurity, each have specific determinants which need to be acknowledged in separate

groups, while taking into consideration the bridges and links in between, which allow the integration of cybersecurity within BIM-FM.

At the strategy layer, the streamlining of the performance-centric determinants and strategic determinants is created to express the vital need for BIM senior-management team competency and cybersecurity oversight on the undertaking of strategic determinants and the development of a security-minded BIM information management strategy.

Research findings illustrate that a security-minded BIM information strategy leads to the buy-in of continuous training and educational programmes that facilitate the continuous improvement and update of both BIM and cybersecurity knowledge and skills, for all business functions of a BIM-FM organisation. Furthermore, a cybersecure BIM information management strategy led by competent leaders and management team who have sufficient oversight of cybersecurity risks, induces a risk-aware culture through a strategic approach to the development of risk management plans and the effective communication of risks to all business functions.

To take into consideration the source domain from which each determinant was derived, BIM and cybersecurity determinants were presented in three layers and bridged to represent the need for effective communication and collaboration between the organisational business functions (i.e., FM and IT teams). Presenting determinants in their own classes also represents the discussions around roles and responsibilities within the empirical results. To exemplify, the cybersecurity-related determinants such as cybersecurity system design, risk-management plans and defined security processes are commonly thought of as determinants which should be picked up by the security specialists, technologists, and IT teams within the FM. However, research findings emphasise the need for an understanding of BIM from a facilities management point of view, to incorporate knowledge of information requirements, BIM-FM roles, BIM-enabled collaboration and FM tasks and operations. Furthermore, BIM-FM determinants such as BIM infrastructure maturity require an understanding of the cyber risks and vulnerabilities of the systems, tools and networks that can be achieved by the incorporation of IT, and the knowledge of security specialists. Hence, effective collaboration ensures that the approach to the BIM infrastructure maturity determinant is not only limited to opting in and investing in the latest BIM infrastructure, but it also includes managing and maintaining the cybersecurity of BIM Infrastructure. The bridge in between the BIM and cybersecurity classes also represents the communication between business functions regarding the processes,

procedures, and risks, to ensure cybersecurity is at the core of all functions. Hence, decisions regarding the BIM implementational tasks including defining BIM-FM task information requirements, monitoring and audit processes, and pre-tender competency evaluation will incorporate cybersecurity.

The successful integration of cybersecurity within a BIM implementation is only fully achieved when the status of implementation is audited and monitored and the feedback is reported to the top decision makers in the strategy-development layer to revise, refine and improve strategies, which leads to an improved implementation of BIM. Furthermore, compliance to cybersecurity rules and regulations should be monitored and the cybersecurity of processes and procedures should be included and considered within the audit trails. Hence, the improvements will encompass the cybersecurity aspect and hence, lead to the identification of the cybersecurity-related shortfalls that can be addressed from the top.

5.4 Conclusion

This chapter provided a discussion of research findings, to discover new knowledge regarding the determinants of a cybersecure BIM-FM. The results led to the formation of a revised research framework, by expanding and improving on the primary research framework developed in chapter 2. The BIMCS-FM framework was hence developed to act as a prompting mechanism for the BIM-FM organisations, to improve cybersecurity and work towards a unified management of cybersecurity and BIM in FM. To ensure the applicability of the framework in BIM-FM organisations, the next Chapter presents the validation of the framework using expert opinion.

Chapter Six: Validation of the research framework

6.1 Introduction

The previous chapter presented a discussion of primary and secondary findings, which led to the revision of the primary research framework. As a result, the BIMCS-FM framework was developed to assist facilities management organisations in the cybersecure implementation of BIM. This chapter aims to validate the BIMCS-FM framework using the opinion of experts. This was facilitated through a set of open-ended questions which were presented in the form of a questionnaire. The validation was conducted to validate the BIMCS-FM framework from two aspects. The first aspect pertained to the stakeholders' understanding of the concepts proposed in the framework, whilst the second aspect was the validation of the framework and its embedded components. The BIMCS-FM framework is a framework which portrays concepts and their interconnections, to act as a prompting mechanism for the facilities managers to implement a cybersecure BIM.

This chapter first presents the method of validation and describes the validation process in detail (section 6.2) and also presents an overview of the questionnaire design (6.3). The results of the validation exercise are presented with respect to the validation objective they fulfil (6.4). Findings were later incorporated into the framework and final revisions were made (6.5). The chapter also provides a summary of the framework deliverables and its contributions (6.6) and is finally concluded in 6.7.

6.2 Validation Using Expert Review

The validation looked into the stakeholder's understanding of the framework and its value in improving the cybersecurity of BIM-FM. The validation also looked into the framework in terms of the concepts embedded including the layers, determinants, and interconnections of layers. The validation provided the views of the experts which either complimented or contradicted the framework and assisted with the final iterations and improvement of the research output.

The validation entails looking into the following aspects:

I. Understanding of concepts and their interconnections within the framework by facilities management organisations.
II. Applicability of the three layers of strategy, implementation, and performance.
III. Applicability of the determinants of cybersecurity integration in BIM-FM.

IV. Validation of the interconnections of the layers within the framework.
V. Value of the framework for improving cybersecurity in BIM-FM organisations.

The collection of expert opinion using a questionnaire was supported by Okoli et al., (2004) and has been proven effective in studies that entail complex questions with notable levels of subjectivity. Therefore, the underpinning reasons for adopting a questionnaire to undertake the validation was:

I. The small size of the expert group simplifies the process, as well as enabling direct communication with the researcher for further clarification or elucidation if required by the experts.
II. The experts would require time to review the determinants description table for each question. Therefore, the questionnaire will provide them with the opportunity to respond to the questions in their own time, rather than spontaneous responses required in other methods such as interviews or focus groups.

The validation was conducted in four stages which included designing the questionnaire, preparing the supporting documents (framework description, determinant description, and consent forms), expert selection, collection, and analysis of responses.

- Stage 1: The first stage entailed preparing a set of questions to address the aim of the validation process. All questions were designed to address the key aspects of the framework validation, either wholly or partially. Considering the nature of the framework, the questionnaire was designed in a way to allow the experts to express their views in depths and details.
- Stage 2: The second stage was to develop a clear description of the framework and the validation process. This description included a table of determinants with a description for each determinant, and an overview of the layers, concepts and connections presented within the framework. The description of the determinants was written using sections 2.5.1.2, 2.5.2.2 and 5.2.
- Stage 3: The third stage involved selecting experts with the necessary knowledge and expertise in the topic under investigation. Validation using an open-ended questionnaire involves selecting a small group of field experts rather than a large number of individuals from a broader range of practitioners or the general members of the

population. This will allow gaining a richer insight into the views of the experts on the framework developed.

This stage was conducted using the method proposed by Pawlowski et al., (2004), to ensure the validity of the expert selection process. It involves identifying the knowledge and expertise required to complete the validation task and selecting experts with the essential knowledge to validate the framework, from an organisational cybersecurity management and/or BIM-FM perspective. Henceforth, experts with experience of managing the cybersecurity of information as part of their role, and/or experience of working in managerial positions at BIM-FM organisations, were contacted for an informal conversation and were questioned on their willingness to participate in the validation study. Finally, experts were selected based on their expertise, availability and participation requirements and a formal invitation was sent to the chosen group of experts. The invitation was in the form of an email, including a brief description of the research and the validation process. The experts who returned their written agreement of participation, were sent the questionnaire and the framework description for validation.

Although the existing literature was not in agreement on the specific number of experts required, a majority of the studies recommended a range between 3 and 20 experts, depending on their availability and the size of the sample used for initial data collection (Fernández-Gómez et al., 2020). Therefore, the validation was conducted using a total of seven experts, from which, five were currently working, or had been previously working, in senior roles within a BIM-FM organisation. The sixth expert was the head of digital asset security for a BIM-FM organisation. The seventh expert was a cybersecurity consultant who had multiple experiences of working with BIM-FM organisations and was also involved in developing cybersecurity guidelines for the AECO stakeholders, in particular, facilities managers and owners. All experts were knowledgeable in BIM and its application to FM.

- Stage 4: The fourth stage was to collect the responses of the experts through email, to analyse and draw conclusion from their suggestions. All the questions requested qualitative feedback as a necessity. Responses to the questions (Appendix 3) were qualitatively analysed. Furthermore, all the experts were informally contacted by the researcher to provide feedback on the validation process. The results of which is discussed in the following sections.

6.3 Questionnaire Design

The questionnaire was designed to address the aspects which were aimed to be validated using expert opinion. These include the stakeholders' understanding of the BIMCS-FM framework and the value it brings to the cybersecurity management of BIM-FM organisations. The questions were designed in an open-ended format to enable the experts to provide rich comments, in response to each question. However, to avoid the responses diverging from the validation focus, all questions were structured to validate the overall structure, layers, determinants, and interconnections between the layers of the framework.

The first two questions addressed the overall structure of the framework (layered structure of determinants), and general opinion of the experts on the terminologies used within the BIMCS-FM. It particularly questioned whether the framework changed their understanding of the concepts proposed in the framework.

The rest of the questionnaire was structured into the different layers of the BIMCS-FM framework, including strategy, implementation, and performance (top level and bottom level) layers. In each layer, the categorisation of determinants for both BIM-FM and cybersecurity was questioned. Furthermore, the experts were asked to comment on the validity of the determinants used within each layer. Finally, the interconnections between the determinants and layers, as proposed in the BIMCS-FM framework was validated using the comments received.

6.4 Validation

The analysis of the comments given by the experts was carried out qualitatively. They were colour coded to distinguish between those that proposed additional recommendations and those that were in opposition to what the framework presents (See Appendix 4). For this cause, responses that gave agreement and positive feedback were coded in green and no further action was then needed for that group. Responses which were not sure about the concept under review but were not expressing opposing views, or responses which were proposing additional suggestions to compliment the presented concept, were coded in yellow. Further elaboration on the matter or additional explanation was required, to address comments coded in yellow. Finally, comments expressing opposing views and suggesting a change in the framework were coded orange. Comments in this category required further action, either by rearrangement or change to the framework, or providing a response in support of the concept.

The comments of experts were reviewed, and those in categories red and yellow were addressed in the analysis. Furthermore, the interdisciplinary and complex nature of the issue also necessitated the importance of providing a response to the recommendations made by the experts. The validation of the framework was structured into the five key aspects of validation, previously acknowledged as the purpose of the validation exercise:

6.4.1 Applicability of the three layers of strategy, implementation, and performance

The first two questions of the questionnaire were designed to address this aspect of validation. Comments illustrated that all experts were familiar with the terminologies used for the determinants and believed they could easily understand the layers and elements of the framework. The feedback showed that:

- All experts expressed their familiarity with the terminologies of the BIMCS-FM framework layers. However, one of them indicated having had no practical experience of the cybersecurity concepts of the framework.
- Another expert raised the point that some small BIM projects might not have the facilities to be approached based on a certain structure, like the one proposed in the BIMCS-FM framework.
- Most experts believed that the concepts and layers of the framework were coherent with their understanding of the BIM and cybersecurity concepts, however, the framework had provided a more detailed view into the determinants required for the integration of cybersecurity in BIM-FM. However, one of them emphasised the need to gain a holistic understanding of the issue of cybersecurity prior to delving into the detail of how it could be managed.

6.4.2 Applicability of the determinants of cybersecurity integration in BIM-FM

Findings regarding the applicability of the determinants included within each layer of the framework is presented below:

1. Strategy Layer

Question 3 was designed to address the applicability of BIM-FM and CS categories to split the determinants in two groups.

- The experts believed that the determinants were applicable to the BIM-FM organisations. In line with this, one of them pointed that for maximising the effect of

the determinants, a balanced decision making is required at board level, to take into consideration the business goals and cybersecurity requirements.

- One of the experts emphasised that the determinants were applicable if there is effective communication between the BIM experts, FM experts and IT experts to implement these determinants.

2. Performance layer

Questions 8 and 10 addressed the performance-related determinants affecting the cybersecure integration of cybersecurity within BIM-FM. Question 8 was designed to collect views on the proposed performance-determinants that affected the undertaking of determinants at the strategy layer (top-layer performance determinants). The comments of the experts illustrated the following:

- All of the experts believed that the performance determinants were important for creating a cybersecurity-minded BIM-FM organisation. However, one of them was sceptical of the need for a CS oversight by the BIM management team if they are taking advice from the cybersecurity team. This concern was inclined towards an over-reliance on cybersecurity/IT specialists and disregarded the importance of balanced decision-making which entailed knowledge and awareness of the cybersecurity context.
- Although experts agreed on the applicability of all determinants, one of them suggested that the performance of those involved in operational activities had a higher influence on the cybersecurity stance of a BIM-FM organisation. Albeit the expert also emphasised that cybersecurity determinants for senior positions was an important enabler of improved performance.
- Another expert also suggested the development of a generic framework to address all digital solutions such as BIM in FM. However, this was outside the scope of this research project.

Question 10 was designed to address performance determinants at functional levels (bottom level performance determinants). Findings from the feedback of the experts was:

- All the experts agreed on the performance determinants at functional levels. One of them suggested that a reward- aware culture might be a better than a risk-aware culture, meaning that employees should be aware of the benefits of creating a balanced approach towards cybersecurity.

3. Implementation Layer

Question 11 addressed the categorisation of determinants into two groups of BIM-FM determinants and cybersecurity (CS) determinants. Findings from the comments of the experts were:

- Experts mostly agreed on the applicability of the determinants in this layer. One insisted on the importance of risk assessment, which is part of the risk management determinant in the framework.
- Some experts considered that these determinants required effective collaboration between the IT and FM teams. The framework has already represented this by the arrows between the two blocks of BIM-FM and CS determinants in the framework.
- One expert also emphasised the importance of externalities which need to be taken into account. The framework has already addressed this by the strategy development determinant, however, it is worth adding this aspect to the determinant's description table, to highlight the importance of considering the external factors while developing a cybersecurity-oriented BIM-FM strategy.

Questions 12 and 13 were designed to address the determinants of cybersecurity integration at the implementation layer within BIM-FM. Findings from the comments of the experts were:

- Experts agreed on the proposed determinants in the implementation layer and further emphasised the importance of a continuous assessment of the competencies of stakeholders rather than a one-off assessment.
- One of the experts suggested including "technical solutions" as a determinant, whilst acknowledging that this was part of the "Defined BIM-FM processes" and given that the focus of this framework was the socio-technical aspects of managing cybersecurity, it will remain as part of the 'defined BIM-FM processes' determinant.
- The comments also emphasised the need to communicate the risk management plans, which was addressed in the definition of a risk-aware culture determinant in the performance layer.
- A number of experts pointed to the role of continuous auditing and monitoring to ensure the plans are being performed in the right way. This is also addressed by the auditing and monitoring of the processes proposed by the framework.

6.4.3 Validation of the interconnections of the layers within the framework

To validate the interconnections between the two groups of BIM-FM and CS determinants at the strategy layer, question 6 points out to the interchangeable effect of the strategic Cybersecurity and BIM-FM determinants. There is the need for effective communication and collaboration between the responsible teams (e.g., IT & FM teams) to implement such determinants in a BIM-enabled FM organisation. Findings from the comments of the experts were:

- Experts all agreed on the interconnections between the two groups of determinants. However, one of the experts suggested having a separate functional unit to manage security and information security by overseeing IT and FM teams. Whilst this suggestion is valid and supported by this research, it is not practical for many of the small and medium companies who do not have sufficient human resources to form such unit. Hence, the BIMCS-FM presents the determinants that contribute to a cybersecurity minded BIM-FM, based on effective communication and collaboration between those responsible of implementing the determinants (IT, FM, BIM, Security teams). Many organisations have already adopted a separate security unit which manages information security by incorporating knowledge and information from FM, BIM, security, and IT perspectives.
- One of the experts stated that in some organisations, there may be external parties carrying out the IT or FM activities and lack of an effective communication with those stakeholders/ service providers may also pose cybersecurity risks. However, the nature of the FM organisations is very different and hence, it is difficult to represent every situation and organisational structure within a framework. The BIMCS-FM is an approach to present the determinants that affect the cybersecurity of BIM-enabled projects within FM and the interactions and connections between the two groups of determinants is emphasised by the need for effective communication and collaboration between those in charge of implementing them. Hence, if any service is outsourced to an external company, there should still be effective communication and collaboration to enable a security-minded implementation of BIM within FM organisations

In addition, question 7 was designed to assess the validity of the relationship between the top-level performance determinants and strategy-layer determinants. BIMCS-FM proposes that the

top-level performance determinants affect the fulfilment of determinants at the strategy layer. The findings from the comments of the experts were:

- They all agreed to the need for the determinants of performance at the top-level for the employment of the strategic determinants. However, their understanding of performance determinants was more inclined towards the performance of functional units and those involved with the operational units rather than those with higher authorities. However, the secondary and primary data collectively shows the importance of a competent management-team and cybersecurity awareness and oversight which would enable cybersecurity-aware decision making. This would incorporate cybersecurity in all processes and procedures. Hence, a top-down approach was suggested.

Furthermore, BIMCS-FM suggests that the development of a cybersecurity-minded organisational BIM strategy leads to the need for cybersecurity embedded-training and educational programs. Question 9 was designed to validate the proposed links between the strategy layer with the deployment of a cybersecurity-minded training and educational program.

- All experts strongly agreed with the vital need for education and training programs for a cybersecurity-oriented BIM-FM.

In addition to the validation of bottom-level performance determinants, question 10 was designed to assess the proposed relationship between the bottom-level performance determinants on the successful implementation of determinants at the implementation layer.

- All experts agreed on the effects of bottom-level performance determinants on the implementation layer.

Moreover, to question the validity of the proposed interconnection between the BIM-FM determinants and CS determinants at the implementation layer, question 14 required the views of the experts on the link proposed by BIMCS-FM. Their feedback illustrated the following findings:

- All experts agreed on the proposed link between the two groups of determinants, but one of them suggested that the collaboration between the two teams should be managed by the security team. Although this was in line with the suggestion in the 1192-5 best practice standard, it was not practical for many organisations (especially SMEs). At the

strategy layer, the inclusion of the cybersecurity-oversight determinant was representative of the importance of such oversight at the managerial level. This could be a separate unit, or part of the managerial team within the organisation. The cybersecurity-oversight determinant was necessary to support security-aware decision making for effective communication between the teams.

- Another suggestion was that the collaboration could be between several organisational teams, alongside CS and FM. What BIM-FM and CS is representing can include as many teams as there are in an organisation. This very much related to the size and structure of every organisation and cannot be generalised. BIM-FM and CS are categories for determinants and many business teams might be responsible for implementing those determinants.

Lastly, BIMCS-FM suggests that the results of the monitoring & auditing should be communicated at every level, to enable improved decision making at the top-level that ultimately feeds improvement into all processes and procedures. This connection was addressed by question 15 and the comments of the experts were requested to validate the links:

- Two of the experts suggested that monitoring and auditing could be optimised using technical solutions to enable real-time monitoring for the detection of intrusion attempts or breaches. However, the BIMCS-FM framework is focused on the non-technical aspects of managing cybersecurity within BIM-FM organisations. The reason is, although technical solutions are widely used within industrial organisations, as with all other digital solutions, they can be breached, disabled, and compromised with the advancements of attacking methods. Furthermore, a large percentage of attacks are undetected, even with the use of varied technical solutions in the different organisations. Hence, BIMCS-FM is focused on continuous monitoring and auditing of compliance as well as the quality of products and services. This can also be carried out using technical solutions, but it should not solely rely on digital solutions.

6.4.4 Understanding of concepts and their interconnections within the framework by facilities management organisations.

The response of experts showed their understanding of what was proposed by the BIMCS-FM, including the constituents and their interconnections. Their comments illustrated that most components of the framework are understandable by the experts. The determinant labelled as ‘organisational modelling of cybersecurity requirements’ was the only exception. Two of the

experts challenged the terminology used to describe this determinant and suggested a change of terminology to assist FM organisations with a better understanding of the framework. Therefore, it can be concluded that the BIMCS-FM was understood and no major changes to the structure or content was required.

6.4.5 Value of the framework for BIM-FM organisations

Question 16 inquired whether the framework was of value to the BIM-enabled FM organisations, by assisting with the integration of cybersecurity within processes and procedures. All experts agreed that the framework was of value to the FM industry. Although one of them mentioned that its application would take time. As for the BIMCS-FM framework, it presented the determinants contributing to the cybersecurity-minded implementation of BIM in FM, so that the FM organisations could implement those determinants at the various levels of strategy, implementation, and performance. As all comments were coded in green, no further action was required by the researcher.

6.5 Revision to Framework

The validation questionnaire provided valuable insight and feedback from experts within the BIM-FM and cybersecurity fields. The responses received fulfilled all aspects of validation which were initially targeted. Their comments also enabled the improvement of the framework through minor justifications. The amendments to the framework following the validation exercise were as follows:

I. Taking “external factors” into account.

One of the experts drew attention to the external factors affecting BIM-FM organisations and how compliance to regulations and standards can bring an adaptive approach towards external influences. The BIMCS-FM framework represents the determinants of BIM Leadership along with standardisation and compliance to regulations, which enables the development of a competent BIM strategy that considers both external and internal factors affecting the organisation as a whole. This comment was taken on board by emphasising the external factors within the definition of the ‘strategy development’ determinant. Hence, the definition of this determinant for the use of the BIMCS-FM framework was changed to: ‘Establishing a strategy that has the extra-organisational factors and intra-organisational business-needs incorporated within and is transferable into the BIM implementation processes & procedures’. This would prompt the facilities management organisations to consider the effects of externalities and

employ a proactive approach towards them by the following of best practice guidelines and standards.

II. Rephrasing and simplifying ‘organisational modelling of information security requirements’ to enable FM organisations to better understand the concepts and terminologies within the framework.

Two of the experts also raised concerns regarding the organisational modelling of security-requirements terminology. One expert stated that the terminology was not clear to FM and should be explained. Another questioned the terminology with respect to its definition and the fact that it doesn’t suggest the need for computational modelling which it implies for the reader. This determinant was commonly accepted by the cybersecurity specialists among the experts; however, it might require a simplification in terms of its label. Hence, the determinant was changed to ‘identification of the organisation’s information security requirements’ to better relate to the definition that is provided for this determinant: ‘Interpretation of organisational information security requirements as part of the organisational information requirements (OIR) document, with respect to organisational goals, value identification, risk tolerance and determining the applicability of cybersecurity controls based on the best-practice guidelines and standards’.

Hence, the BIMCS-FM framework was adjusted in definition and terminology to accommodate the views of the experts and improve on its value for the facilities management organisations. The adjustments were coloured in red in the framework (Figure 15) and table of definitions (Table 9):

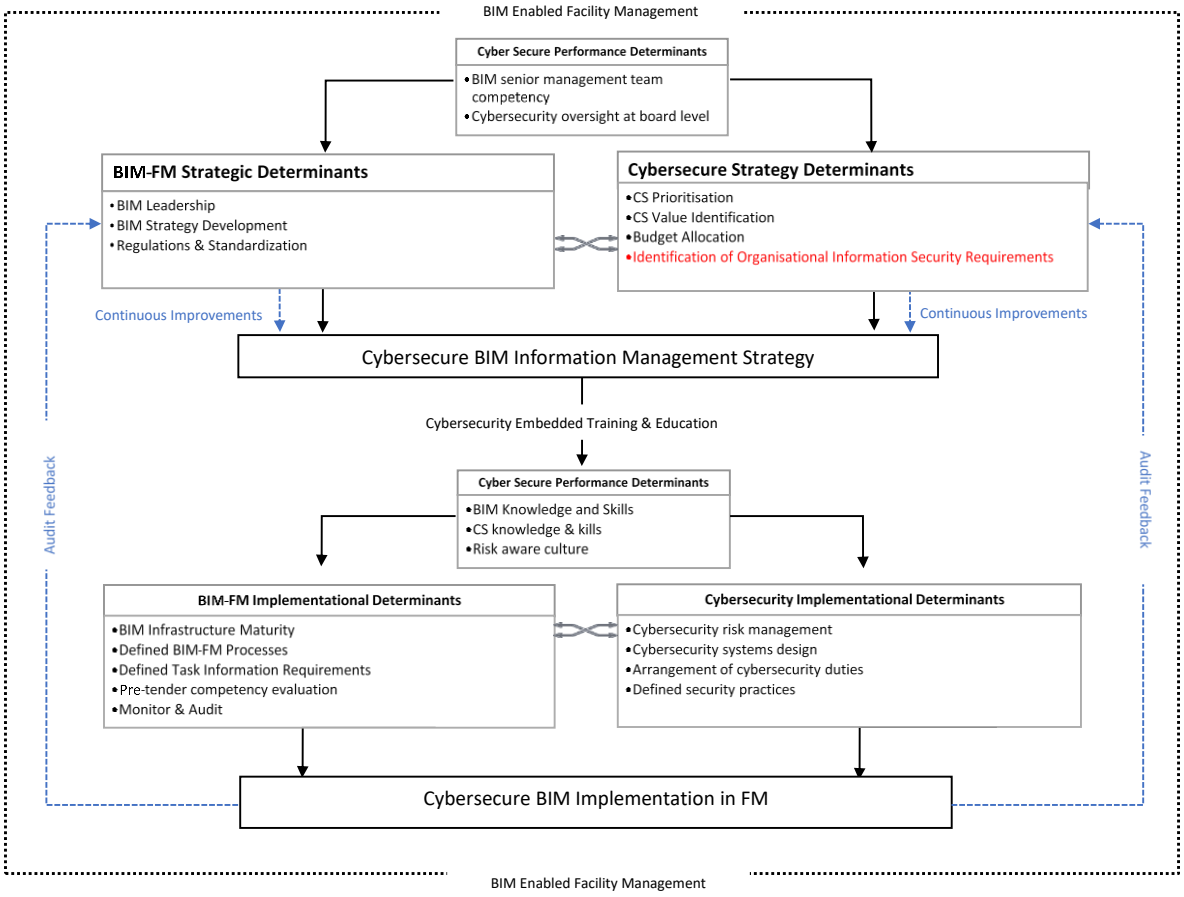


Figure 15- Validated BIMCS-FM Framework

Table 9- Validated BIMCS-FM Determinants' Description

	Determinants	Description
Strategic Layer	BIM Leadership	BIM Leadership is to translate the purpose of BIM implementation (BIM vision, mission, objectives) into actionable strategies that enable organisational implementation of BIM.
	BIM Strategy Development	Establishing a strategy that has the extra-organisational factors and intra-organisational business needs incorporated within and is transferable into the BIM implementational processes & procedures
	Regulations & Standardisation	BIM strategy is developed upon the best-practice guidelines & standards and incorporated into implementational and performance improvement processes and procedures.
	CS Prioritisation	Strategic prioritisation of cybersecurity initiatives, planning and investment based on organisational needs, to ensure cybersecurity is embedded into the BIM-FM strategy.
	CS Value Identification	Identification of the value of information and assets and the potential losses in case of a cyber-attack. Value can be monetary or non-monetary (reputation, trust, etc)
	Budget Allocation	Allocation of financial resources to facilitate implementation of organisational strategies
	Identifying Organisational Information Security Requirements	Interpretation of organisational information security requirements as part of the organisational information requirements (OIR) doc, with respect to organisational goals, value identification, risk tolerance and determining the applicability of cybersecurity controls based on the best-practice guidelines and standards

Implementation Layer	BIM Infrastructure Maturity	Adoption of fit for purpose BIM infrastructure managed and maintained by continuous updates and assessments to ensure technological excellence.
	Defined BIM-FM Processes	BIM-FM working processes including data sharing, interaction between stakeholders and communication are formally documented and regulated based on best-practice guidelines and standards.
	Defined Task Information Requirements	Development of the Employers Information Requirement document (EIR) to reflect on the OIR specifications and set out the BIM Execution Plan (BEP) projection.
	Stakeholder's Capability Evaluation	Evaluation of supply-chain capabilities in fulfilling the requirements of EIR, addressing their information management competencies and IT and human resource capabilities.
	Monitor & Audit	Continuous monitoring of processes and auditing of performance to ensure adherence with strategic rules and regulations, leading to continuous improvement of processes and deliverables quality during the whole life cycle of a project.
	Cybersecurity Risk Management	To identify, analyse, evaluate, and treat a cybersecurity risks to the digital information of a BIM-enabled FM organisation.
	Reliable Cybersecurity System Design	Designing reliable systems to protect digital data, based on the information security requirements and risk management capabilities.
	Defined Security Processes	Defining and formalising processes and procedures to manage and maintain cybersecurity, as well as enabling process improvements by monitoring and measuring performance.
	Arrangement of cybersecurity Duties	Assigning and documenting the accountability of employees towards the cybersecurity of information.
Performance Layer	BIM Senior Management Team Competency	The extent to which the BIM management team support the adoption and implementation of BIM, by standardisation of processes and procedures and providing sufficient resources and facilities.
	BIM Knowledge & Skills	Continuous training and education to ensure up to date BIM knowledge and skills for all employees.
	Cybersecurity Oversight at Board Level	Managing and motivating cyber security at the strategy level through leveraging, influencing, and ensuring full support from senior-management teams as well as effective collaboration of IT & business management teams for the integration of cyber-security initiatives.
	Cybersecurity Knowledge & Skills	Continuous training and education to supply employees with the latest capabilities required for full compliance with organisational cybersecurity regulations, processes, and procedures.
	Risk-Aware Culture	Establishing a culture where all employees value, promote and practice cybersecurity procedures to protect the security of digital information with respect to the security requirements set out as part of the risk management process.

6.6 Framework Beneficiaries

The BIMCS-FM framework is an intellectual construct that presents the determinants of a cybersecure implementation of BIM in facilities management organisations. The connections of the determinants guide the facilities management organisations to adopt a cybersecurity-oriented approach to the implementation of BIM. The transformation of the primary framework through outlining the amendments support the following deliverables:

I. The framework advocates an apprehension of the need for an organisational shift that fosters a mature implementation of BIM information management that has

cybersecurity at its core.

II. Defines baseline determinants of cybersecurity integration within BIM-enabled FM to address the shortfalls and limitations that challenge the integration.

III. Accentuates the role of people and process in managing and maintaining a cybersecure BIM-FM.

IV. Establishes a framework for bridging cybersecurity and BIM determinants, in support of a cybersecure BIM in various layers of strategy, implementation and performance in FM.

With respect to the above deliverables, this framework assists the senior management teams in BIM-FM organisations, to embed cybersecurity in their strategies, processes, and employee ways of working. Due to the varying structure of the BIM-FM organisations, the senior management team may consist of various roles that are labelled differently within each organisation. Hence, this research focuses on those involved in the top managerial decision making, who have an overview of the strategic, implementational and performance aspects of BIM in FM. Therefore, this framework encourages the incorporation of cybersecurity considerations within all business functions of a BIM enabled facilities management organisation.

The application of this framework requires fundamental transformations within a BIM-enabled organisation, to be able to build up the knowledge, skill set, awareness and culture that is required for a cybersecurity-minded implementation of BIM. Furthermore, the implementation of the concepts proposed in various levels of strategy, implementation, and performance, should be approached through the development of process models that would be fit for purpose within various BIM-enabled FM organisations of different sizes, structures, and different sectors (e.g., education, industry, health, etc.). Investigation into the ways in which a single determinant can be approached within a BIM-FM organisation is required to identify the process that is required for implementation of a determinant such as “BIM infrastructure maturity” or “risk aware culture”. Hence, the BIMCS-FM framework assists with providing an insight into the concepts that should be considered for a cybersecurity-oriented implementation of BIM within FM. It can also be considered as a key source of information for the development of work plans, and process models within the industry.

6.7 Conclusion

The comments and feedback of experts demonstrated a general consensus on the value that the BIMCS-FM framework brings to FM organisations, by proposing a structured approach to improving cybersecurity in various levels of strategy, implementation, and performance. The inclusion of determinants and their interconnections within each level emphasise the key contributing factors to cybersecurity management and enables FM to tackle the issue with a better understanding of the required competencies and capabilities. Hence, the BIMCS-FM framework fulfils the aim of the research, by acting as a prompting mechanism which will lead to a more cybersecure management of BIM-enabled facilities management organisations.

The validation exercise enabled the researcher to validate the model and improve on the minor issues with the terminologies and phrasings. The views of the experts were relatively homogeneous and did not indicate any major divergence of thought and opinion. The minor terminology issues which were brought up by a couple of experts were incorporated in the framework and amended accordingly. A final version of the research framework was developed to inform the cybersecurity-related considerations within BIM-enabled FM (Figure 15).

Chapter Seven: Conclusion

7.1 Introduction

In achieving the aim of the research, previous chapters showed the formation, validation and development of the final research framework using the theoretical and empirical findings. The secondary data collection revealed a number of determinants contributing to a cybersecure BIM-enabled facilities management, which were used to construct a primary research framework (chapter 2). The empirical findings (chapter 4) from the thematic analysis of interviews with industry professionals were later synchronised with the theoretical findings, leading to the formation of the BIMCS-FM framework (Chapter 5), based on the primary framework construct. The BIMCS-FM framework was validated and finalised (chapter 6) in response to the research question, of how cybersecurity can be improved in the implementation of BIM in FM.

This chapter presents the research findings to demonstrate evidence of the fulfilment of the research question, aim and objectives. It demonstrates the way in which the findings respond to the research question, by discussing the contributions, potential implications, and limitations of each phase of the research. Section 7.2 illustrates the way the findings address the research objectives and their contribution to the achievement of the research aim. Sections 7.3 outlines the theoretical and practical contributions, followed by the limitations and future studies in sections 7.4 and 7.5 respectively.

7.2 Results attribution to research objectives

Four research objectives were proposed to reach the main aim of the research (chapter 1). Through the review of the literature in BIM (Sections 2.2), the first research objective was achieved, which highlighted the issue of cybersecurity in various phases of the BIM lifecycle (Section 2.2.6). To take further steps towards the achievement of the research aim, the second research objective was fulfilled by investigating the risk factors affecting cybersecurity in BIM-enabled facilities management, by reviewing the literature in BIM-enabled facilities management and cybersecurity in the digital built-environment (Section 2.3, 2.4). Objective three was partially fulfilled through the development of the primary research framework, including the BIM and cybersecurity determinants that contribute towards the improved cybersecurity of a BIM-FM organisation (Section 2.6). The primary research framework was further revised and expanded based on the empirical data, collected using interviews. The revised framework fulfilled the third research objective by identifying determinants of a

cybersecure BIM-FM (chapter 5,6). Finally, the fourth research objective was fulfilled by validating and finalising the BIMCS-FM framework (chapter 6), to act as a prompting mechanism assists BIM-enabled facilities management organisations in improving their cybersecurity status. The sub-sections below provide a synthesis of findings, pertaining to the accomplishment of each research objective and its contribution to the achievement of the research aim.

7.2.1 Research Objective I –To critically explore the cybersecurity risks in various phases of a BIM lifecycle.

The first research objective was achieved by a review of the literature for BIM and cybersecurity, with a particular focus on the various phases of a BIM lifecycle. Findings illustrated that during the in-use phase of the project, facilities managers were responsible for managing and maintaining both the digital and physical aspects of the facilities, in collaboration with various stakeholders. Hence, large volumes of as-built and as-maintained information were shared with a large group of stakeholders, with differing processes and procedures for the managing and handling of digital information. Thus, robust information-management processes in this phase of a BIM project are required to accomplish the full potential of BIM in FM. This directed the research to focus on the cybersecurity management in BIM-FM organisations.

7.2.2 Research Objective II- To identify the risk factors affecting cybersecurity in BIM-FM organisations.

To identify the challenges of managing cybersecurity in BIM-FM organisations, section 2.3 explored the application of BIM in various task areas of FM. Findings illustrated the significance of the availability of accurate and up to date information, of the facility to achieve the benefits of BIM in FM. Findings also unveiled the challenges associated with the application of BIM in FM. These challenges related to the strategy, implementation, and performance layers of an organisation and had the people, processes, and technology at their core. Section 2.3.3 showed how the challenges in the implementation of BIM in FM resulted in an increased cybersecurity vulnerability. Therefore, it was concluded that overcoming BIM implementation challenges can minimise the cybersecurity vulnerabilities.

To further explore these vulnerabilities, section 2.4 considered the cybersecurity threats, risks, and their impacts on BIM-FM organisations. Based on the cybersecurity triad, a risk matrix was developed to represent how an infringement of data confidentiality, availability and

integrity may compromise the BIM benefits in various task areas of a facilities management organisation (section 2.4.3). The findings illustrate that cybersecurity threats may target people, process or technology-related vulnerabilities within the strategy, implementation, and performance layers of an organisation. However, current measures were seldom focused on the technical cybersecurity measures, whilst also neglecting to consider measures that minimise the people-related and process-related vulnerabilities.

Results conclude that effective cybersecurity management with particular focus on people and processes is required, to overcome the BIM challenges that lead to a higher cybersecurity vulnerability in BIM-FM organisations. Therefore, a mature implementation of BIM that includes cybersecurity considerations is required in BIM-FM organisations.

7.2.3 Research objective III- To determine the requirements of a cybersecure implementation of BIM in FM.

In fulfilling the third research objective, this study sought to investigate what the existing resources propose for overcoming cybersecurity vulnerabilities raised by the challenges identified in BIM-FM (section 2.3.3). In doing so, BIM maturity models were explored to identify people-related and process-related determinants, contributing to a cybersecure BIM in FM. Succar's BIM maturity model (Succar, 2010) and CIC BIM maturity model (Construction Industry Council, 2013) were selected for their focus on the managerial and social aspects of BIM as well as their applicability to FM (section 2.5.1). Thus, BIM determinants applicable to FM organisations were extracted from the two models. The review of BIM maturity models was indicative of a lack of focus on the people and process aspects of cybersecurity and a sole focus on maintaining infrastructure security and ensuring technology excellence. Therefore, the investigations were directed to resources in organisational cybersecurity management to extract the people-related and process related determinants of a cybersecure organisation. The cybersecurity determinants were identified from the review of secondary data including best-practice guidelines, standards, and peer-reviewed journals. A primary research framework was developed to represent the integration of cybersecurity determinants with BIM-FM determinants (section 2.6), to overcome the strategic, implementational and performance challenges.

The primary framework was further expanded and revised based on the empirical findings from interviews with industry professionals. As a result, the third research objective was met by the

assimilation of theoretical and empirical findings, which also contributed to the fulfillment of the final objective (i.e., development of a framework).

7.2.4 Research objective IV. To develop and validate a framework that supports an improved integration of cybersecurity considerations in BIM-FM organisations.

Empirical findings from the interviews demonstrated the interconnections between the BIM-FM and cybersecurity determinants. Hence, the BIMCS-FM framework was developed, portraying the determinants contributing to a cybersecure BIM in FM together with their interconnections (section 5.3). The determinants included BIM-FM and cybersecurity determinants to enable the integration of cybersecurity in the strategy-setting, implementation, and performance of BIM-enabled FM organisations. The interconnections between the BIM-FM and cybersecurity determinants demonstrated the need for effective communication and collaboration between those responsible for the deployment of each determinant. The need for the collaboration was to overcome the isolated approach to cybersecurity management and enable informed decision making for both cybersecurity and BIM-FM tasks.

To finalise the development of the BIMCS-FM framework and achieve the fourth research objective, a validation exercise was conducted using a review by experts of the BIMCS-FM framework (chapter 6). The validation was carried out using an open-ended questionnaire, from which minor modifications were applied to the framework. The experts suggested minor alterations in the terminology to avoid confusion and misunderstanding amongst the FM organisations. The findings from the validation also emphasised the need to consider the external factors affecting the cybersecurity of a BIMFM organisation. Therefore, this aspect was highlighted in the definition of the 'strategy development' determinant and hence, the definition was finalised as 'establishing a strategy that has the extra-organisational factors and intra-organisational business needs incorporated within and is transferable into the BIM implementation processes & procedures. It was further concluded that the BIMCS-FM framework (section 6.4.5) was a valuable prompting mechanism for facilities management organisations to improve the cybersecurity in their organisations.

7.3 Contributions

The contributions of this research are structured as contributions to theory and practice. The theoretical contributions entail the assimilation of knowledge from the two key domains of BIM-FM and cybersecurity, to bridge the existing knowledge gap within the literature.

Furthermore, contributions to the industry involves assisting the facilities management organisations to achieve a cybersecure implementation of BIM.

7.3.1 Theoretical Contributions

- Eliciting process-related and people-related considerations for cybersecurity within the BIM-FM:

Following a critical review of cybersecurity and the implementation of BIM in FM, it was highlighted that BIM and cybersecurity were often coupled technologically with a limited emphasis on people-related and process-related complexities. As demonstrated by the findings from the review of the literature, these complexities increase the vulnerability of FM to cybersecurity attacks. Therefore, a risk matrix (section 2.4.3) mapping cybersecurity breaches within BIM-enabled FM was developed to support portraying the necessity of acknowledging people and process related vulnerabilities. The risk matrix showed how a cyber-attack compromises the benefits of BIM in FM. Considering that the accomplishment of potential BIM benefits in FM is supported by maturity models, this can inform future determinants within BIM maturity models. This is because existing maturity models within BIM acknowledge cybersecurity as part of the BIM infrastructure maturity, which propose an isolated technology-dependent approach to the management of cybersecurity. Therefore, by the integration of cybersecurity in strategic, implementational and performance determinants, this study sought to emphasise the people-related and process-related cybersecurity considerations and inform the future BIM maturity models to support the cybersecure adoption and implementation of BIM.

7.3.2 Contributions to Practice

- Developing a BIMCS-FM framework that acts as a prompting mechanism for cybersecurity considerations within BIM-enabled FM:

The BIMCS-FM framework was developed to unite the two domains of BIM-FM and cybersecurity from a people and process perspective (Figure 15). The determinants presented within this framework create a contemporary body of knowledge for academics and researchers in the fields of cybersecurity management, BIM, and FM to explore the implementation of each determinant in BIM-enabled organisations with varying characteristics (e.g., size, industry sector, etc.). The literature highlighted that is often the responsibility of the IT teams to manage expectations regarding cybersecurity. This tended to happen in isolation from the FM teams

and hence incurring a lack of cybersecurity oversight in the decisions made by the FM teams. Similarly, the management of cybersecurity was carried out with little consideration for the BIM-FM operational needs, which create challenges in managing access to the information required by various stakeholders. Therefore, the development of the BIMCS-FM framework acts as a prompting mechanism for the BIM-FM organisation, to integrate cybersecurity considerations within the strategic, implementational and performance related aspects of their organisation.

Furthermore, the BIMCS-FM framework highlights the role of people and processes, recognising the part played by robust processes, to facilitate, manage and maintain the digital technologies supporting BIM. Hence, it assists senior managers and decision makers in BIM-FM organisations to transform their approach to cybersecurity management from reactive to proactive, by conceptualising the determinants which FM should invest in for an improved cybersecurity.

7.4 Limitations

Throughout this research project, attention was given to build in a high level of quality into the processes of data collection, data analysis and reporting of the findings. However, a PhD journey entails limitations brought about by time and resources which inherently affects the research. The scope of the research targets three main concepts of BIM, cybersecurity, and FM, where gathering in-depth knowledge and expertise in all three domains is a challenge that needs to be overcome by the researcher alone. Researcher's background and level of knowledge and expertise in each domain significantly affects the project's approach and the resources required. The exploratory review of literature conducted at the beginning of this research was to gain understanding of the three domains and the way they influence one another.

The preliminary review of literature also illustrated another limitation with respect to the availability of resources that address the aim of the research focusing on the people and process aspects of cybersecurity in BIM enabled FM. This issue was tackled through using secondary data from the two domains of BIM and cybersecurity, followed by a qualitative analysis of secondary data based on the findings from the literature review in BIM enabled facilities management. Although the available resources in BIM and cybersecurity did not specifically address the issue of cybersecurity in BIM enabled facilities management organisations, they were used develop a knowledge block that addresses cybersecurity in BIM-FM. This knowledge block was primarily presented as the primary research framework and was later enhanced and modified using empirical findings resulted from thematic analysis of 25 semi-structured interviews with industry professionals.

As with most interpretive and qualitative research, debates around the researcher-bias and/or respondent-bias will also come into play. The adoption of BIM within FM organisations is still at its initial stages, therefore, the implementation of BIM is mostly project-based and ad-hoc, depending on the financial resources of the client and the level of understanding of the benefits of BIM. In these situations, the main focus is on the modelling aspects of BIM (which are usually desirable from the point-of-view of the client), rather than the more necessary and fundamental changes needed in the way that information is managed and maintained. Therefore, those selected to take part in this study were from organisations which were at different levels of BIM adoption. This meant that their interview responses were dependent on

their experience, knowledge, and the way they applied BIM in their day-to-day work. This can be referred to as respondent-bias which needed to be taken into account in a qualitative study.

Another potential limitation of this study was the researcher-bias, which is a common threat to interpretive studies within qualitative research. This study has paid careful attention to avoid this, by constantly comparing the findings from the empirical data analysis with the findings from the secondary data analysis and existing literature. A validation exercise was also carried out to assess the validity of the findings and to ensure the researcher-bias did not affect the results.

7.5 Future Studies

- Future studies will seek to investigate the concept of cybersecurity risks in various types of BIM-FM organisations, across all phases of a BIM project. Assimilation of findings in section 2.2.6 illustrated that a cybersecurity breach negatively effects all phases of a BIM project. Therefore, further exploration is required to capture the extent of impact in various scenarios, including various stakeholders, various types of projects, BIM maturity, and many more influential factors affecting the risk impact across the lifecycle of a BIM project.
- Based on the review of literature, the BIM-FM specific risk matrix in section 2.4.3 maps potential cybersecurity risk impact on the BIM benefits for various areas of FM. This was carried out by combining of the findings from the review of literature in the two distinct domains of BIM-FM and cybersecurity, which sets out the foundations for further research into the probabilities and severity of risk, using empirical data to validate or expand on the developed risk matrix.
- The BIMCS-FM framework developed as the main output of this research, presents a number of determinants that contribute to an improved cybersecurity in BIM-enabled FM organisations. Future research could explore the means for implementing each determinant depending on the characteristics of organisations, (such as size, sector, clients, etc.) by developing process models that can be applied in various organisations. This will also enable the evaluation of this framework using empirical data, following a full investment in the determinants proposed.
- Future research can also explore the application of the BIMCS-FM framework in all BIM-enabled organisations across other phases of a BIM project. Although the BIM-FM determinants were selected for facilities management organisations, the framework has the potential to be adjusted for the use of other BIM stakeholders. This requires

future explorations into the applicability of the framework in other phases of a BIM project, the suitability of the determinants for other phases and how it would be adjusted to meet the requirements of all stakeholders.

7.6 Final Thoughts

The advancement of digital technologies such as the Building Information Modelling in the built environment has led to an increased cybersecurity risk to the facilities management organisations and the facilities they manage and maintain. It has been evident that organisations are keener on the digitisation aspects of BIM adoption, rather than focusing on the digitalisation of their modus operandi. A matter which yields lower BIM maturity in terms of the people and process aspects of BIM implementation, and inherently leads to a lower immunity to cybersecurity breach. Thus, BIM enabled FM organisations should take a proactive approach towards a mature adoption and implementation of BIM that has cybersecurity considerations at its core. This requires a competent approach to the strategic, procedural and performance requirements of the adoption and implementation of a cybersecure BIM in FM, that is reinforced by upskilling and knowledge management of the employees both in senior management positions and the operational teams. This is also in line with the latest publication on driving transformational change in the digital built environment, where it emphasises the need for an organisational change to accomplish the benefits associated with the adoption of technologies in the built environment (Shelbourn and Underwood, 2021).

"A multidisciplinary approach to competency-based management across sectors, disciplines, professions, etc., matters more than targeting productivity improvement through rapidly changing technologies"(Shelbourn and Underwood, 2021)

List of References

Abbasnejad, B., Nepal, M.P., Ahankoob, A., Nasirian, A. and Drogemuller, R. (2020), "Building Information Modelling (BIM) adoption and implementation enablers in AEC firms: a systematic literature review", *Architectural Engineering and Design Management*, available at:https://doi.org/10.1080/17452007.2020.1793721.

Abdelmohsen, S., Lee, J. and Eastman, C. (2011), "Automated cost analysis of concept design BIM models", *Designing Together: CAADFutures 2011 - Proceedings of the 14th International Conference on Computer Aided Architectural Design*.

Abdullah, S.A., Sulaiman, N., Latiffi, A.A. and Baldry, D. (2013), "Integration of Facilities Management (FM) Practices with Building Information Modeling (BIM)", *Ist FPTP Postgraduate Seminar 2013, 23 December 2013*, No. December, available at: http://eprints.uthm.edu.my/5416/1/1st_FPTP_Postgrad_Seminar_2013_U.pdf.

Abdullah, S.A., Sulaiman, N., Latiffi, A.A. and Baldry, D. (2015), "Building Information Modeling (BIM) from the perspective of Facilities Management (FM) in Malaysia", *Proceedings of the 25th International Business Information Management Association Conference - Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 2015*.

Abie, H. (2019), "Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems", *International Symposium on Medical Information and Communication Technology, ISMICT*, available at:https://doi.org/10.1109/ISMICT.2019.8743670.

Acohido, B. (2015), *Improving Detection , Prevention and Response with Improving Detection , Prevention and Response with Security Maturity Modeling*, *SANS Institute*.

Adams, W.C. (2015), "Conducting Semi-Structured Interviews", *Handbook of Practical Program Evaluation: Fourth Edition*, available at:https://doi.org/10.1002/9781119171386.ch19.

Adegbesan, J.A. and Higgins, M.J. (2011), "The intra-alliance division of value created through collaboration", *Strategic Management Journal*, available at:https://doi.org/10.1002/smj.872.

AEC (UK) Committee. (2012), "AEC (UK) BIM Protocol v2.0 - Implementing UK BIM Standards for the Architectural, Engineering and Construction industry.", *Aec (Uk)*.

Ahmad, A. M., Demian, P., and Price, A.D. (2012), “BIM implementation plans: a comparative analysis.”, *Proceedings of 28th Annual ARCOM.*, Association of Researchers in Construction, Edinburgh, UK, pp. 33–42.

Ahmad Zawawi, Z., Ismail, F., Kamaruddin, N. and Kurdi, M.K. (2014), “The core services of the facilities management based company in Malaysia”, *MATEC Web of Conferences*, available at:https://doi.org/10.1051/matecconf/20141501016.

AIA. (2013), “Guide, Instructions and Commentary to the 2013 AIA Digital Practice Documents”, *BIM-Guide*.

Akbarieh, A., Jayasinghe, L.B., Waldmann, D. and Teferle, F.N. (2020), “BIM-based end-of-lifecycle decision making and digital deconstruction: Literature review”, *Sustainability (Switzerland)*, Vol. 12 No. 7, available at:https://doi.org/10.3390/su12072670.

Akcamete, A., Akinci, B. and Garrett, J.H. (2019), “Potential utilization of building information models for planning maintenance activities”, *EG-ICE 2010 - 17th International Workshop on Intelligent Computing in Engineering*.

Al-Janabi, S. and Al-Shourbaji, I. (2016), “A Study of Cyber Security Awareness in Educational Environment in the Middle East”, *Journal of Information and Knowledge Management*, available at:https://doi.org/10.1142/S0219649216500076.

Al-rimy, B.A.S., Maarof, M.A. and Shaid, S.Z.M. (2018), “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2018.01.001.

Alavi, S.H. and Forcada, N. (2019), “BIM LOD for facility management tasks”, *Proceedings of the 2019 European Conference on Computing in Construction*, available at:https://doi.org/10.35490/ec3.2019.187.

Alkasisbeh, M.R. and Abudayyeh, O. (2018), “Building asset management system: A performance evaluation approach”, *IISE Annual Conference and Expo 2018*.

Allmark, P., Boote, J., Chambers, E., Clarke, A., McDonnell, A., Thompson, A. and Tod, A.M. (2009), “Ethical Issues in the Use of In-Depth Interviews: Literature Review and Discussion”, *Research Ethics*, available at:https://doi.org/10.1177/174701610900500203.

Almarabeh, T. and AbuAli, A. (2010), “A general framework for E-government: Definition

maturity challenges, opportunities, and success", *European Journal of Scientific Research*.

Alreshidi, E., Mourshed, M. and Rezgui, Y. (2017), "Factors for effective BIM governance", *Journal of Building Engineering*, Elsevier, Vol. 10, pp. 89–101.

Amaio, T.E. (2009), *Exploring and Examining the Business Value of Information Security: Corporate Executives' Perceptions*, *Northcentral University*.

Amatsari, J.S., Bayar, M.S., Aziz, Z., Tezel, A., Arayici, P.Y., Biscaya, S., Wang, Y., *et al.* (2017), "ORGANISATIONAL INFORMATION REQUIREMENTS (OIR) Estate Directorate : Project Control Framework", *BIM Task Group*.

Amin, Z. (2019), "A practical road map for assessing cyber risk", *Journal of Risk Research*, available at:https://doi.org/10.1080/13669877.2017.1351467.

Aminzade, M. (2018), "Confidentiality, integrity and availability – finding a balanced IT framework", *Network Security*, available at:https://doi.org/10.1016/S1353-4858(18)30043-6.

Anderson, E.E. and Choobineh, J. (2008), "Enterprise information security strategies", *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2008.03.002.

Anderson, J. (2003), "Why we need a new definition of information security", *Computers & Security*, Vol. 22, pp. 308–313.

Andronache, A. (2019), "Aligning cybersecurity management with enterprise risk management in the financial industry", Brunel University London.

Apostolopoulos, C., Halikias, G., Maroukian, K. and Tsaramirsis, G. (2016), "Facilitating organisational decision making: a change risk assessment model case study", *Journal of Modelling in Management*, available at:https://doi.org/10.1108/JM2-05-2014-0035.

Aram, S., Eastman, C. and Sacks, R. (2013), "Requirements for BIM platforms in the concrete reinforcement supply chain", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2013.01.013.

Arayici, Y. and Aouad, G. (2011), "Building information modelling (BIM) for construction lifecycle management", *Construction and Building: Design, Materials, and Techniques*, No. October 2010, pp. 99–117.

Archer, M., Bhaskar, R., Collier, A., Lawson, T. and Norrie, A. (2013), *Critical Realism: Essential Readings*, *Critical Realism: Essential Readings*, available at:https://doi.org/10.4324/9781315008592.

Archer, M.S. (2016), "Reconstructing Sociology: The Critical Realist Approach", *Journal of Critical Realism*, available at:https://doi.org/10.1080/14767430.2016.1191809.

ARCHIBUS. (2013), "Driving Business Transformation for Real Estate, Infrastructure, and Facilities Management", available at: https://www.archibus.net/index.cfm?circuit=document&template_id=1493 (accessed 11 November 2020).

Architectural, U.K. (2015), "Practical implementation of BIM for the UK architectural, engineering and construction (AEC) industry", *AEC (UK) BIM TEchnology Protocol. v2.1.1*.

Arslan, M., Riaz, Z., Kiani, A.K. and Azhar, S. (2014), "Real-time environmental monitoring, visualization and notification system for construction H&S management", *Journal of Information Technology in Construction*, available at:https://doi.org/10.5840/agstm201454111.

Ashcraft, H.W. (2008), "Building information modeling: a framework for collaboration", *Society of Construction Law International Conference*.

Ashworth, S., Tucker, M. and Druhmann, C. (2016), "The Role of FM in Preparing a BIM Strategy and Employer's Information Requirements (EIR) to Align with Client Asset Management Strategy", *15th EuroFM Research Symposium*.

Ashworth, S., Tucker, M., Druhmann, C. and Kassem, M. (2016), "Integration of FM expertise and end user needs in the BIM process using the Employer's Information Requirements (EIR)", *Proceedings of CIB World Building Congress*, Vol. 5 No. May, pp. 1–12.

Atkin, B., & Brooks, A. (2015), *Total Facility Management*, John Wiley & Sons.

Autodesk. (2020), "Insight, Operation and Maintenance", available at: https://knowledge.autodesk.com/support/insight/learn-explore/caas/simplecontent/content/operations-and-maintenance.html (accessed 30 August 2020).

Axelrod, C.W. (2013), “Managing the risks of cyber-physical systems”, *9th Annual Conference on Long Island Systems, Applications and Technology, LISAT 2013*, available at:https://doi.org/10.1109/LISAT.2013.6578215.

Azhar, S., Hein, M., & Sketo, B. (2008), “Building Information Modeling (BIM): benefits, risks, and challenges”, *Proceedings of the 43rd ASC National Annual Conference*, The Associated Schools of Construction (ASC), Flagstaff, AZ, pp. 1–11.

Azhar, S., Nadeem, A., Mok, J. Y., & Leung, B.H. (2008), “Building Information Modeling (BIM): a new paradigm for visual interactive modeling and simulation for construction projects”, *First International Conference on Construction in Developing Countries (ICCIDC–I)*, Advancing and Integrating Construction Education, Research & Practice, Karachi, Pakistan, pp. 435–446.

Azhar, S. (2011), “Building information modeling (BIM): Trends, benefits, risks, and challenges for the AEC industry”, *Leadership and Management in Engineering*, available at:https://doi.org/10.1061/(ASCE)LM.1943-5630.0000127.

Azzouz, A., Shepherd, P. and Copping, A. (2016), “THE EMERGENCE OF BUILDING INFORMATION MODELLING ASSESSMENT METHODS (BIM-AMs)”, *Integrated Design Conference at University of Bath*.

Bailey, T., Kaplan, J.M. and Rezek, C. (2015), “Repelling the cyberattackers”, *McKinsey Quarterly*.

Baker, E.W. (2014), “A Model for the Impact of Cybersecurity Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan”, *Information Technology for Development*, available at:https://doi.org/10.1080/02681102.2013.832131.

Baldwin, A. and Bordoli, D. (2014), *Handbook for Construction Planning and Scheduling*, *Handbook for Construction Planning and Scheduling*, available at:https://doi.org/10.1002/9781118838167.

Bandi, D. (2019), “BIM Vs. CAD Files: What’s The Difference?”, 19 February, available at: https://blog.thomasnet.com/cad-vs-bim-files (accessed 23 April 2021).

Barbarosoglu, B.V. and Arditi, D. (2019), “A System for Early Detection of Maintainability Issues Using BIM”, *Advances in Informatics and Computing in Civil and Construction*

Engineering, available at:https://doi.org/10.1007/978-3-030-00220-6_40.

Barbosa, M.J., Pauwels, P., Ferreira, V. and Mateus, L. (2016), "Towards increased BIM usage for existing building interventions", *Structural Survey*, available at:https://doi.org/10.1108/SS-01-2015-0002.

Barlette, Y. and Fomin, V. V. (2009), "The adoption of information security management standards: A literature review", *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, available at:https://doi.org/10.4018/978-1-60566-326-5.ch006.

Barrett, P. and Baldry, D. (2003), *Facilities Management: Towards Best Practice*, *Facilities Management*.

Baskerville, R. and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Logistics Information Management*, available at:https://doi.org/10.1108/09576050210447019.

Bayuk, J.L. (2012), "Cyber Attacks", *Computers & Security*, available at:https://doi.org/10.1016/j.cose.2011.12.008.

Bazjanac, V. (2008), "IFC BIM-based methodology for semi-automated building energy performance simulation", *CIB-W78 25th International Conference on Information Technology in Construction*.

Beautement, A., Sasse, M.A. and Wonham, M. (2009), "The compliance budget: Managing security behaviour in organisations", *Proceedings New Security Paradigms Workshop*, available at:https://doi.org/10.1145/1595676.1595684.

Becerik-Gerber, B., Jazizadeh, F., Li, N. and Calis, G. (2012a), "Application Areas and Data Requirements for BIM-Enabled Facilities Management", *Journal of Construction Engineering and Management*, available at:https://doi.org/10.1061/(asce)co.1943-7862.0000433.

Becerik-Gerber, B., Jazizadeh, F., Li, N. and Calis, G. (2012b), "Application Areas and Data Requirements for BIM-Enabled Facilities Management", *Journal of Construction Engineering and Management*, Vol. 138 No. 3, pp. 431–442.

Bechtold, B.L. (1997), "Toward a participative organizational culture: evolution or revolution?", *Empowerment in Organizations*, available

at:https://doi.org/10.1108/14634449710168750.

Becker, F. and Steele, F. (1990), "The total workplace", *Facilities*, available at:https://doi.org/10.1108/eum0000000002099.

Beecham, S., Hall, T., Britton, C., Cottee, M. and Rainer, A. (2005), "Using an expert panel to validate a requirements process improvement model", *Journal of Systems and Software*, available at:https://doi.org/10.1016/j.jss.2004.06.004.

Bello, S.M. (2012), "Impact of Ethical Leadership on Employee Job Performance", *International Journal of Business and Social Science*.

Berkman, H., Jona, J., Lee, G. and Soderstrom, N. (2018), "Cybersecurity awareness and market valuations", *Journal of Accounting and Public Policy*, available at:https://doi.org/10.1016/j.jaccpubpol.2018.10.003.

Van Berlo, L. and Hendriks, H. (2012), "BIM QUICKSCAN: BENCHMARK OF BIM PERFORMANCE IN THE NETHERLANDS", *CIB W78 2012: 29th International Conference*.

Van Berlo, L.A.H.M., Beetz, J., Bos, P., Hendriks, H. and Van Tongeren, R.C.J. (2012), "Collaborative engineering with IFC: New insights and technology", *EWork and EBusiness in Architecture, Engineering and Construction - Proceedings of the European Conference on Product and Process Modelling 2012, ECPPM 2012*.

Bew, M., and Richards, M. (2008), "BIM Maturity Model", *Construct IT Autumn 2008 Members' Meeting*, Brighton, UK.

Bhattacherjee, A. (2012), *Social Science Research: Principles, Methods, and Practices, Book 3*.

BIM Portal. (2020), "Stage 2 - Concept - Plain Language Questions", available at: https://bimportal.scottishfuturestrust.org.uk/level2/stage/2/plqs (accessed 1 September 2020).

BIM Task Group. (2012), "The Government Soft Landings Policy", available at: http://www.bimtaskgroup.org/gsl policy.

BIM United. (2020), "BIM Maturity Levels Explained- Level 0, Level 1, Level 2, Level 3", available at: https://www.united-bim.com/bim-maturity-levels-explained-level-0-1-2-3/

(accessed 30 August 2020).

Bin-Abbas, H. and Bakry, S.H. (2014), "Assessment of IT governance in organizations: A simple integrated approach", *Computers in Human Behavior*, available at:https://doi.org/10.1016/j.chb.2013.12.019.

Binesmael, M., Li, H. and Lark, R. (2018), "Meta-standard for collaborative BIM standards: an analysis of UK BIM level 2 standards", *Working Conference on Virtual Enterprises*, Springer, pp. 661–668.

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015), "Cyber resilience – Fundamentals for a definition", *Advances in Intelligent Systems and Computing*, available at:https://doi.org/10.1007/978-3-319-16486-1_31.

Bloomberg, L.D. and Volpe, M. (2018), "Completing your qualitative dissertation: A road map from beginning to end", Sage Publications.

Bohnert, A., Gatzert, N., Hoyt, R.E. and Lechner, P. (2019), "The drivers and value of enterprise risk management: evidence from ERM ratings", *European Journal of Finance*, available at:https://doi.org/10.1080/1351847X.2018.1514314.

Borky, J.M. and Bradley, T.H. (2018), "Protecting Information with Cybersecurity", *Effective Model-Based Systems Engineering*, pp. 345–404.

Borum, R., Felker, J., Kern, S., Dennesen, K. and Feyes, T. (2015), "Strategic cyber intelligence", *Information and Computer Security*, available at:https://doi.org/10.1108/ICS-09-2014-0064.

Boslaugh, S. (2009), "An Introduction to Secondary Data Analysis", *Secondary Data Sources for Public Health*, Cambridge University Press, Cambridge, pp. 1–11.

Bowen, B.M., Devarajan, R. and Stolfo, S. (2011), "Measuring the human factor of cyber security", *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, available at:https://doi.org/10.1109/THS.2011.6107876.

Bowen, P., Hash, J., Wilson, M., Gutierrez, C.M. and Jeffrey, W. (2006), "Information Security Handbook: A Guide for Managers", *NIST Special Publication 800-100*.

Boxall, E. (2015), "Common Data Environment (CDE): What you need to know for starters."

Boyes, H. (2015a), "Security, Privacy, and the Built Environment", *IT Professional*, Institute

of Electrical and Electronics Engineers (IEEE), Vol. 17 No. 3, pp. 25–31.

Boyes, H. (2015b), “and the Built Environment”, IEEE, pp. 25–31.

Boyes, H. (2015c), “Security, privacy, and the built environment”, *IT Professional*, available at:https://doi.org/10.1109/MITP.2015.49.

Brackney, R. and Anderson, R. (2004), *Understanding the Insider Threat, Proceedings of the March 2004 Workshop*.

Bradford, A. (2017), “Deductive Reasoning vs. Inductive Reasoning”, *Live Science*.

Braumann, E.C. (2018), “Analyzing the role of risk awareness in enterprise risk management”, *Journal of Management Accounting Research*, available at:https://doi.org/10.2308/jmar-52084.

Braun, V. and Clarke, V. (2012), “Thematic analysis.”, *APA Handbook of Research Methods in Psychology, Vol 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological.*, available at:https://doi.org/10.1037/13620-004.

Brewer, R. (2016), “Ransomware attacks: detection, prevention and cure”, *Network Security*, available at:https://doi.org/10.1016/S1353-4858(16)30086-1.

British Institue of Facilities Management. (2012), “BIM and FM : Bridging the gap for success”, *F M L e a d e r s F o r u M : D i s c u s s i o n P a P e r o c T o B e r 2 0 1 2*.

British Standards Insitution. (2015), “PAS 1192-5:2015 - Specification for security-minded building information modelling, digital built environments and smart asset management”, *Bsi*.

British Standards Institution (BSI). (2012), “BS ISO 21500:2012(E). Guidance on project management”, *International Standard*.

Bryman, A. (2016), *Social Research Methods - Alan Bryman - Oxford University Press*, *Oxford University Press*.

Bryman, A., Becker, S. and Sempik, J. (2008), “Quality criteria for quantitative, qualitative and mixed methods research: A view from social policy”, *International Journal of Social Research Methodology*, available at:https://doi.org/10.1080/13645570701401644.

BSI. (2007), “BS ISO/IEC 27006:2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security

management systems", available at: https://shop.bsigroup.com/ProductDetail/?pid=000000000030148919 (accessed 30 November 2020).

BSI. (2013a), "PAS 1192-2:2013", *BSI Standards Publication*.

BSI. (2013b), *PAS555:2013 Cyber Security Risk – Governance and Management – Specification, PAS 555:2013 Cyber Security Risk - Government and Mangement - Specification*.

BSI. (2016), "Collaborative production of architectural, engineering and construction information – Code of practice", *Astm*.

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlstrom, P., Henke, N., *et al.* (2017), "Investing in an Age of Technology Disruption Background Information", *McKinsey Global Institute*.

BuildingSMART. (2010), *Constructing the Business Case. Building Information Modelling, British Standards Institution*.

Butcher, J. (2019), *Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview*.

Cabinet Office. (2012), "Government Property Unit The Government Soft Landings Policy", *Cabinet Office*.

Cabric, M. (2015), "Confidentiality, Integrity, and Availability", *Corporate Security Management*, available at:https://doi.org/10.1016/b978-0-12-802934-3.00011-1.

Calder, Alan ; Watkins, S. (2019), *IT Governance An Internation Guide to Data Security and ISO27001/ISO27002- OU Edition, 7th Edition, KoganPage*.

Calvin Kam, Fischer, M., Bedrick, J., Widney, J. and Rinella, T. (2013), "VDC and BIM Scorecard", *JOURNAL OF THE NATIONAL INSTITUTE OF BUILDING SCIENCES*.

Capps, P. (2019), "Interpretivism", *Concepts for International Law: Contributions to Disciplinary Thought*, available at:https://doi.org/10.4337/9781783474684.00041.

Caralli, R. and Wilson, W. (2004), "The challenges of security management", *Pittsburgh, PA: CERT, Software Engineering …*.

Carbonari, G., Stravoravdis, S. and Gausden, C. (2018), "Improving FM task efficiency

through BIM: a proposal for BIM implementation", *Journal of Corporate Real Estate*, available at:https://doi.org/10.1108/JCRE-01-2017-0001.

Carlsson, S.A. (2009), "Critical realism", *Handbook of Research on Contemporary Theoretical Models in Information Systems*, available at:https://doi.org/10.4018/978-1-60566-659-4.ch004.

Carnero, M.C. and Gómez, A. (2017), "A multicriteria model for optimization of maintenance in thermal energy production systems in hospitals: A case study in a Spanish hospital", *Sustainability (Switzerland)*, available at:https://doi.org/10.3390/su9040493.

Carreira, P., Castelo, T., Gomes, C.C., Ferreira, A., Ribeiro, C. and Costa, A.A. (2018), "Virtual reality as integration environments for facilities management: Application and users perception", *Engineering, Construction and Architectural Management*, available at:https://doi.org/10.1108/ECAM-09-2016-0198.

Carter, R.B., Sree, N. and Daniel, N. (1991), "Strategic Planning for Information Systems", *Journal of Research on Computing in Education*, available at:https://doi.org/10.1080/08886504.1991.10782009.

Casadesus-Masanell, R. and Ricart, J.E. (2010), "From strategy to business models and onto tactics", *Long Range Planning*, available at:https://doi.org/10.1016/j.lrp.2010.01.004.

Cassano, M. and Trani, M.L. (2017), "LOD Standardization for Construction Site Elements", *Procedia Engineering*, available at:https://doi.org/10.1016/j.proeng.2017.08.062.

Centre for Digital Built Britain. (2018), "FAQ for ISO 19650 Transition", *University of Cambridge*.

CERT, U.K. (2015), "Cyber-security Information Sharing Partnership (CiSP)".

Chen, L. and Luo, H. (2014), "A BIM-based construction quality management model and its applications", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2014.05.009.

Chen, L., Shi, P., Tang, Q., Liu, W. and Wu, Q. (2020), "Development and application of a specification-compliant highway tunnel facility management system based on BIM", *Tunnelling and Underground Space Technology*, available at:https://doi.org/10.1016/j.tust.2019.103262.

Chen, Y. and Kamara, J.M. (2011), “A framework for using mobile computing for information management on construction sites”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2011.01.002.

Cheng, H.G. and Phillips, M.R. (2014), “Secondary analysis of existing data: opportunities and implementation”, *Shanghai Archives of Psychiatry*, available at:https://doi.org/10.11919/j.issn.1002-0829.214171.

Cho, H. (2002), *A Study on the Relationship of Construction Information Documents Control for Automatic Generation of Construction Documents*, Ajou University.

Chronopoulos, M., Panaousis, E. and Grossklags, J. (2017), “An Options Approach to Cybersecurity Investment”, *IEEE Access*, available at:https://doi.org/10.1109/ACCESS.2017.2773366.

Chunduri, S., Kreider, R. and Messner, J.I. (2013), “A case study implementation of the bim planning procedures for facility owners”, *AEI 2013: Building Solutions for Architectural Engineering - Proceedings of the 2013 Architectural Engineering National Conference*, available at:https://doi.org/10.1061/9780784412909.068.

CIC. (2013), “Building information model (BIM) protocol”, *Construction Industry Council, London*, p. 15.

Cisco. (2018), “Cisco 2018 Annual Cybersecurity Report”, *Cisco 2018 Annual Cybersecurity Report*, p. 68.

Clarke, R. (2015), “The prospects of easier security for small organisations and consumers”, *Computer Law & Security Review*, Elsevier, Vol. 31 No. 4, pp. 538–552.

CMU. (2003), “System Security Engineering Capability Maturity Model (SSE-CMM)”, *Proceedings of the 19th International Conference on Software Engineering ICSE 97*.

Cohen, D. and Crabtree, B. (2006), “Semi-structured Interviews Recording Semi-Structured interviews”, *Qualitative Research Guidelines Project*.

Construction Industry Council. (2013), *CIC BIM Protocol: BUILDING INFORMATION MODEL (BIM) PROTOCOL. Standard Protocol for Use in Projects Using Building Information Models, First Edition*.

Cooke-Davies, T.J. (2004), “Measurement of organizational maturity: What are the relevant

questions about maturity and metrics for a project-based organization to ask, and what do these imply for project management research?", *Project Management Journal*.

COSO. (2017), *Enterprise Risk Management. Integrating with Strategy and Performance, The Committee of Sponsoring Organizations of the Treadway Commission*.

Costello, D. (2011), "Incorporating community governance: planning sustainable energy security", *The International Journal of Environmental, Cultural, Economic & Social Sustainability*, Common Ground Publishing, Vol. 7.

Couce-Vieira, A., Insua, D.R. and Kosgodagan, A. (2020), "Assessing and forecasting cybersecurity impacts", *Decision Analysis*, available at:https://doi.org/10.1287/DECA.2020.0418.

Cox, A., Townsend, M., Publishing, I.C.E., Company, T., Industry, A., Review, L., Latham, S.M., *et al.* (2016), "Strategic Procurement in Construction Towards better practice in the management of construction supply chains", *International Journal of Project Management*.

Cresswell, J.W. and Cresswell, J.D. (2018), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, *Research Defign: Qualitative, Quantitative, and Mixed Methods Approaches*.

Creswell, J.W. (2015), *Mapping the Developing Landscape of Mixed Methods Research*, *SAGE Handbook of Mixed Methods in Social & Behavioral Research*, SAGE Publications, Inc., available at:https://doi.org/10.4135/9781506335193.n2.

Creswell, J.W. and Poth, C.N. (2016), *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, Sage publications.

Crotty, M. (1998), "Introduction: The research process", *The Foundations of Social Research: Meaning and Perspective in the Research Process*, pp. 1–17.

Cui, L., Xie, G., Qu, Y., Gao, L. and Yang, Y. (2018), "Security and privacy in smart cities: Challenges and opportunities", *IEEE Access*, available at:https://doi.org/10.1109/ACCESS.2018.2853985.

Culot, G., Fattori, F., Podrecca, M. and Sartor, M. (2019), "Addressing Industry 4.0 Cybersecurity Challenges", *IEEE Engineering Management Review*, available at:https://doi.org/10.1109/EMR.2019.2927559.

Czmoch, I. and Pękala, A. (2014), “Traditional design versus BIM based design”, *Procedia Engineering*, available at:https://doi.org/10.1016/j.proeng.2014.12.048.

Dakhil, A. (2017), *Building Information Modelling (BIM) Maturity-Benefits Assessment Relationship Framework for UK Construction Clients*, University of Salford, UK.

Dakhil, A., Underwood, J. and Al Shawi, M. (2019), “Critical success competencies for the BIM implementation process: UK construction clients”, *Journal of Information Technology in Construction*.

Daniotti, B., Pavan, A., Lupica Spagnolo, S., Caffi, V., Pasini, D. and Mirarchi, C. (2020), “Benefits and Challenges Using BIM for Operation and Maintenance”, *Springer Tracts in Civil Engineering*, available at:https://doi.org/10.1007/978-3-030-32889-4_7.

Davtalab, O. (2017), “Benefits of real-time data driven BIM for FM departments in operations control and maintenance”, *Congress on Computing in Civil Engineering, Proceedings*, Vol. 0, American Society of Civil Engineers (ASCE), pp. 202–210.

Dawood, Nashwan NWhole Lifecycle Information Flow Underpinned By Bim: Technology, Process, P. and P. and Vukovic, V. (2015), “Whole Lifecycle Information Flow Underpinned By Bim: Technology, Process, Policy and People”, *2nd International Conference on Civil and Building Engineering Informatics*, Vol. 7 No. 696114, pp. 1–7.

Dawood, S., Lord, R. and Dawood, N. (2009), “Development of a visual whole life-cycle energy assessment framework for built environment”, *Proceedings - Winter Simulation Conference*, available at:https://doi.org/10.1109/WSC.2009.5429263.

Delany, S. (2019), “What is Uniclass 2015?”, *Classification*.

Demian, P. and Walters, D. (2014), “The advantages of information management through building information modelling”, *Construction Management and Economics*, available at:https://doi.org/10.1080/01446193.2013.777754.

Denzin, N.K. and Lincoln, Y.S. (2000), “Introduction: The discipline and practice of qualitative research”, *Handbook of Qualitative Research (2nd Edition)*.

Dixon-Woods, M., Agarwal, S., Jones, D., Young, B. and Sutton, A. (2005), “Synthesising qualitative and quantitative evidence: A review of possible methods”, *Journal of Health Services Research & Policy*, SAGE Publications, Vol. 10 No. 1, pp. 45–53.

Doneda, D. and Almeida, V.A.F. (2015), “Privacy Governance in Cyberspace”, *IEEE Internet Computing*, available at:https://doi.org/10.1109/MIC.2015.66.

Dourish, P. and Anderson, K. (2006), “Collective information practice: Exploring privacy and security as social and cultural phenomena”, *Human-Computer Interaction*, available at:https://doi.org/10.1207/s15327051hci2103_2.

Dzazali, S. and Hussein Zolait, A. (2012), “Assessment of information security maturity”, *Journal of Systems and Information Technology*, available at:https://doi.org/10.1108/13287261211221128.

Eadie, R., Browne, M., Odeyinka, H., McKeown, C. and McNiff, S. (2013), “BIM implementation throughout the UK construction project lifecycle: An analysis”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2013.09.001.

Eadie, R., Mclernon, T. and Patton, A. (2015), “AN INVESTIGATION INTO THE LEGAL ISSUES RELATING TOBUILDING INFORMATION MODELLING (BIM)”, *RICS COBRA AUBEA 2015*.

Ebinger, M. and Madritsch, T. (2012), “A classification framework for facilities and real estate management: The Built Environment Management Model (BEM2)”, *Facilities*, available at:https://doi.org/110.1108/02632771211208477.

Edirisinghe, R., London, K.A., Kalutara, P. and Aranda-Mena, G. (2017), “Building information modelling for facility management: Are we there yet?”, *Engineering, Construction and Architectural Management*, available at:https://doi.org/10.1108/ECAM-06-2016-0139.

Edmondson, V., Cerny, M., Lim, M., Gledson, B., Lockley, S. and Woodward, J. (2018), “A smart sewer asset information model to enable an ‘Internet of Things’ for operational wastewater management”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2018.03.003.

Edwards, M.M. (2018), “Identifying factors contributing towards information security maturity in an organization”.

Ekelhart, A., Fenz, S. and Neubauer, T. (2009), “AURUM: A framework for information security risk management”, *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*, available

at:https://doi.org/10.1109/HICSS.2009.82.

Ekstedt, M. and Sommestad, T. (2009), "Enterprise architecture models for cyber security analysis", *2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009*, available at:https://doi.org/10.1109/PSCE.2009.4840267.

Ellis, B.A. (2006), *Building Information Modeling: An Informational Tool for Stakeholders*.

Enoma, A., Allen, S. and Enoma, A. (2009), "Airport redesign for safety and security: Case studies of three scottish airports", *International Journal of Strategic Property Management*, available at:https://doi.org/10.3846/1648-715X.2009.13.103-116.

Eriksson, P. and Kovalainen, A. (2008), "Qualitative research materials", *SR Methods, Qualitative Methods in Business Research*, pp. 78–97.

Escobar-Pérez, J. and Cuervo-Martínez, Á. (2008), "Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización", *Avances En Medición*.

Evans, K. and Reeder, F. (2010), "A Human Capital Crisis in Cybersecurity", *Technical Proficiency Matters*.

EY. (2017), "Public sector innovation. From ideas to actions", *Ernst & Young*.

Fahrenkrog, S., Abrams, F., Haeck, W.P. and Whelbourn, D. (2003), "Project Management Institute's Organizational Project Management Maturity Model (OPM3^{TM})", *PMI North America Conference*.

Fairholm, M.R. and Card, M. (2009), "Perspectives of strategic thinking: From controlling chaos to embracing it", *Journal of Management and Organization*, available at:https://doi.org/10.5172/jmo.837.15.1.17.

Farell, M. and Gallagher, R. (2015), "The Valuations Implications of ERM Maturity", *The Journal of Risk and Insurance*.

FBIFM, J.M.W. (2010), "Facilities manager's desk reference", Wiley Online Library.

Federal Emergency Management Agency. (2003), *Multi-Hazard Loss Estimation Methodology, Earthquake Model, HAZUS-MH MR4 Technical Manual, National Institute of Building Sciences and Federal Emergency Management Agency (NIBS and FEMA)*.

Fernández-Gómez, E., Martín-Salvador, A., Luque-Vara, T., Sánchez-Ojeda, M.A., Navarro-

Prado, S. and Enrique-Mirón, C. (2020), “Content Validation through Expert Judgement of an Instrument on the Nutritional Knowledge, Beliefs, and Habits of Pregnant Women”, *Nutrients*, MDPI, Vol. 12 No. 4, p. 1136.

Flick, U., Foster, J. and Caillaud, S. (2015), “Researching social representations”, *The Cambridge Handbook of Social Representations*, Cambridge University Press Cambridge, UK, Vol. 3 No. 1, pp. 64–80.

Foss, N.J. and Michailova, S. (2009), *Knowledge Governance: Processes and Perspectives*, *Knowledge Governance: Processes and Perspectives*, available at:https://doi.org/10.1093/acprof:oso/9780199235926.001.0001.

Gale, N.K., Heath, G., Cameron, E., Rashid, S. and Redwood, S. (2013), “Using the framework method for the analysis of qualitative data in multi-disciplinary health research”, *BMC Medical Research Methodology*, available at:https://doi.org/10.1186/1471-2288-13-117.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011), “Dimensions of cyber-attacks: Cultural, social, economic, and political”, *IEEE Technology and Society Magazine*, available at:https://doi.org/10.1109/MTS.2011.940293.

Gao, X. and Pishdad-Bozorgi, P. (2019), “BIM-enabled facilities operation and maintenance: A review”, *Advanced Engineering Informatics*, available at:https://doi.org/10.1016/j.aei.2019.01.005.

Garrote, P.R. and del Carmen Rojas, M. (2015), “La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada”, *Revista Nebrija de Lingüística Aplicada a La Enseñanza de Lenguas*, No. 18, pp. 124–139.

Gerber, M. and Von Solms, R. (2005), “Management of risk in the information age”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2004.11.002.

Gerber, M., Von Solms, R. and Overbeek, P. (2001), “Formalizing information security requirements”, *Information Management and Computer Security*, available at:https://doi.org/10.1108/09685220110366768.

Ghaffarianhoseini, A., Tookey, J., Ghaffarianhoseini, A., Naismith, N., Azhar, S., Efimova, O. and Raahemifar, K. (2017a), “Building Information Modelling (BIM) uptake: Clear

benefits, understanding its implementation, risks and challenges", *Renewable and Sustainable Energy Reviews*, Elsevier BV, Vol. 75, pp. 1046–1053.

Ghaffarianhoseini, A., Tookey, J., Ghaffarianhoseini, A., Naismith, N., Azhar, S., Efimova, O. and Raahemifar, K. (2017b), "Building Information Modelling (BIM) uptake: Clear benefits, understanding its implementation, risks and challenges", *Renewable and Sustainable Energy Reviews*, available at:https://doi.org/10.1016/j.rser.2016.11.083.

Ghosh, A., Hosseini, M. R., Edwards, D., Kassem, M., & Matteo-Garcia, M. (2019), "Use cases for the Internet of Things (IoT) in the construction sector: Lessons from leading industries", *CIB W78 2019: Proceedings of 36th CIB (International Council for Research and Innovation in Building and Construction) W78 2019 Conference*, CIB (International Council for Research and Innovation in Building and Construction), pp. 1–8.

Giel, B. and Issa, R.R.A. (2013), "Quality and maturity of BIM implementation in the AECO industry", *Applied Mechanics and Materials*, Vol. 438–439, pp. 1621–1627.

Glantz, C., Somasundaram, S., Mylrea, M., Underhill, R., & Nicholls, A. (2016), *Evaluating the Maturity of Cybersecurity Programs for Building Control Systems*.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015), "The impact of information sharing on cybersecurity underinvestment: A real options perspective", *Journal of Accounting and Public Policy*, available at:https://doi.org/10.1016/j.jaccpubpol.2015.05.001.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2016), "Investing in Cybersecurity: Insights from the Gordon-Loeb Model", *Journal of Information Security*, available at:https://doi.org/10.4236/jis.2016.72004.

Gourlis, G. and Kovacic, I. (2017), "Building Information Modelling for analysis of energy efficient industrial buildings – A case study", *Renewable and Sustainable Energy Reviews*, available at:https://doi.org/10.1016/j.rser.2016.02.009.

Gray, D.E. (2014), *Theoretical Perspectives and Research Methodologies, Doing Research in the Real World*.

Griffin, P.H. (2019), "Advances in Human Factors in Cybersecurity", *Advances in Intelligent Systems and Computing*.

Groff, R. (2004), *Critical Realism, Post-Positivism And The Possibility Of Knowledge*, *Critical Realism, Post-Positivism And The Possibility Of Knowledge*, available at:https://doi.org/10.4324/9780203417270.

Grytting, I., Svalestuen, F., Lohne, J., Sommerseth, H., Augdal, S. and Lædre, O. (2017), "Use of LoD Decision Plan in BIM-projects", *Procedia Engineering*, available at:https://doi.org/10.1016/j.proeng.2017.07.217.

Gu, N. and London, K. (2010), "Understanding and facilitating BIM adoption in the AEC industry", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2010.09.002.

Gu, N., Vishal, S., Kerry, L., Brankovic, L. and Claudelle, T. (2008), "Adopting building information modeling (BIM) as collaboration platform in the design industry", *CAADRIA 2008 - The Association for Computer-Aided Architectural Design Research in Asia: Beyond Computer-Aided Design*.

Guest, G., MacQueen, K. and Namey, E. (2014), *Applied Thematic Analysis*, *Applied Thematic Analysis*, available at:https://doi.org/10.4135/9781483384436.

Guillen, A.J., Crespo, A., Gómez, J., González-Prida, V., Kobbacy, K. and Shariff, S. (2016), "Building Information Modeling as Assest Management Tool", *IFAC-PapersOnLine*, available at:https://doi.org/10.1016/j.ifacol.2016.11.033.

Guillen, D., Gomez, D., Hernandez, I., Charris, D., Gonzalez, J., Leon, D. and Sanjuan, M. (2020), "Integrated methodology for industrial facilities management and design based on FCA and lean manufacturing principles", *Facilities*, available at:https://doi.org/10.1108/F-03-2019-0040.

Hakim, C. (1982), "Secondary analysis and the relationship between official and academic social research", *Sociology*, available at:https://doi.org/10.1177/0038038582016001005.

HARDIN, B. (2009), *BIM and Construction Management - Proven Tools, Methods, and Workflows*, *Igarss 2014*.

Harding, J. (2018), *Qualitative Data Analysis: From Start to Finish*, Sage.

Haynes, S.N., Richard, D. and Kubany, E.S. (1995), "Content validity in psychological assessment: A functional approach to concepts and methods.", *Psychological Assessment*, American Psychological Association, Vol. 7 No. 3, p. 238.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *Journal of Strategic Information Systems*, available at:https://doi.org/10.1016/j.jsis.2011.06.001.

Henderson, A. (2019), "The CIA Triad: Confidentiality, Integrity, Availability", *Panmore Institute*.

HM Goverment. (2015), "Small businesses: What you need to know about cyber security", *HM Government*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf (accessed 24 April 2021).

Hoang, G. V, Vu, D.K.T., Le, N.H. and Nguyen, T.P. (2020), "Benefits and challenges of BIM implementation for facility management in operation and maintenance face of buildings in Vietnam", *IOP Conference Series: Materials Science and Engineering*, Vol. 869, available at:https://doi.org/10.1088/1757-899X/869/2/022032.

Honti, R. and Erdélyi, J. (2018a), "Possibilities of bim data exchange", *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM*, Vol. 18 No. 2.2, pp. 923–930.

Honti, R. and Erdélyi, J. (2018b), "Possibilities of bim data exchange", *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM*, available at:https://doi.org/10.5593/sgem2018/2.2/S09.117.

Hopkin, P. (2014), "Achieving enhanced organisational resilience by improved management of risk: Summary of research into the principles of resilience and the practices of resilient organisations", *Journal of Business Continuity & Emergency Planning*, Henry Stewart Publications, Vol. 8 No. 3, pp. 252–262.

Hopkin, P. (2018), *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, Kogan Page Publishers.

House, S.O., Ballesty, S., Mitchell, J., Drogemuller, R., Schevers, H., Linning, C., Singh, G., *et al.* (2007), *Adopting BIM for Facilities Management: Solutions for Managing the Sydney Opera House, CRC for Construction Innovation Participants*.

Hu, W.F. (2008), "Information Lifecycle Modeling Framework for Construction Project

Lifecycle Management.", *International Seminar on Future Information Technology and Management Engineering*, pp. 372–375.

Hu, Z.Z., Tian, P.L., Li, S.W. and Zhang, J.P. (2018), "BIM-based integrated delivery technologies for intelligent MEP management in the operation and maintenance phase", *Advances in Engineering Software*, available at:https://doi.org/10.1016/j.advengsoft.2017.08.007.

Huang, K. and Pearlson, K. (2019), "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture", *Proceedings of the 52nd Hawaii International Conference on System Sciences*, available at:https://doi.org/10.24251/hicss.2019.769.

Huber, M., Kowalski, S., Nohlberg, M. and Tjoa, S. (2009), "Towards automating social engineering using social networking sites", *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, available at:https://doi.org/10.1109/CSE.2009.205.

Humphreys, E. (2008), "Information security management standards: Compliance, governance and risk management", *Information Security Technical Report*, available at:https://doi.org/10.1016/j.istr.2008.10.010.

Hussain, A., Mohamed, A. and Razali, S. (2020), "A Review on Cybersecurity", *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, ACM, available at:https://doi.org/10.1145/3386723.3387847.

Hutchins, G. (2018), *ISO 31000: 2018 Enterprise Risk Management*, Greg Hutchins.

Hutchins, M.J., Bhinge, R., Micali, M.K., Robinson, S.L., Sutherland, J.W. and Dornfeld, D. (2015), "Framework for Identifying Cybersecurity Risks in Manufacturing", *Procedia Manufacturing*, available at:https://doi.org/10.1016/j.promfg.2015.09.060.

Hyrkäs, K., Appelqvist-Schmidlechner, K. and Oksa, L. (2003), "Validating an instrument for clinical supervision using an expert panel", *International Journal of Nursing Studies*, available at:https://doi.org/10.1016/S0020-7489(03)00036-1.

Iden, J., Methlie, L.B. and Christensen, G.E. (2017), "The nature of strategic foresight research: A systematic literature review", *Technological Forecasting and Social Change*, available at:https://doi.org/10.1016/j.techfore.2016.11.002.

IET. (2013), *Resilience and Cyber Security of Technology in the Built Environment*,

Birmingham, available at: www.theiet.org/resources/standards/ cyber-buildings.cfm?origin=pr.

Ignatow, G. and Mihalcea, R. (2018), "Thematic Analysis, Qualitative Data Analysis Software, and Visualization", *Text Mining: A Guidebook for the Social Sciences*, available at:https://doi.org/10.4135/9781483399782.n7.

Ikerd, W., Merrifield, D., Vandezande, J., Cichonski, W., Dellaria, R., Filkins, B., Karakas, M., *et al.* (2013), "Level of Development Specification", *Bim Forum*.

Ilter, D. and Ergen, E. (2015), "BIM for building refurbishment and maintenance: current status and research directions", *Structural Survey*, available at:https://doi.org/10.1108/SS-02-2015-0008.

Indiana University. (2009), "Building Information Modeling (BIM): Guidelines and Standards For Architects, Engineers, And Contractors", *Indiana Architech Office*.

Information security forum. (2005), "The standard good practice for information security", *Information Security Forum*.

ISACA. (2012a), *Enabling Processes, Cobit 5*.

ISACA. (2012b), *A Business Framework for the Governance and Management of Enterprise IT, Trust And Partnership*.

ISACA. (2014), "Cobit 5", *Isaca*.

Isikdag, U. (2012), "Design patterns for BIM-based service-oriented architectures", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2012.04.013.

ISO/IEC27010. (2012), "BSI Standards Publication Information technology — Security techniques — information security management for inter-sector and inter-organizational", *BSI Standards Publication Information*.

Jeong, Y.S., Eastman, C.M., Sacks, R. and Kaner, I. (2009), "Benchmark tests for BIM data exchanges of precast concrete", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2008.11.001.

Johansson, E., Ekstedt, M. and Johnson, P. (2006), "Assessment of enterprise information security the importance of information search cost", *Proceedings of the Annual Hawaii International Conference on System Sciences*, available

at:https://doi.org/10.1109/HICSS.2006.67.

Joint Task Force. (2018), *Risk Management Framework for Information Systems and Organizations:*, *NIST Special Publication - 800 Series*.

Kabanda, G. (2018), "A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations", *Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations. AJMECS*.

Kam, C., Senaratna, D., Mckinney, B. and Xiao, Y. (2014), "The VDC Scorecard: Formulation and Validation", *CIFE Working Paper*.

Kaplan, S. (2011), "Strategy and PowerPoint: An inquiry into the epistemic culture and machinery of strategy making", *Organization Science*, available at:https://doi.org/10.1287/orsc.1100.0531.

Karlshøj, J., See, R. and Davis, D. (2012), "An Integrated Process for Delivering IFC Based Data Exchange", *BuildingSMART International*.

Kassem, M., Kelly, G., Dawood, N., Serginson, M. and Lockley, S. (2015a), "BIM in facilities management applications: A case study of a large university complex", *Built Environment Project and Asset Management*, Vol. 5 No. 3, pp. 261–277.

Kassem, M., Kelly, G., Dawood, N., Serginson, M. and Lockley, S. (2015b), "BIM in facilities management applications: A case study of a large university complex", *Built Environment Project and Asset Management*, available at:https://doi.org/10.1108/BEPAM-02-2014-0011.

Kassem, M. and Li, J. (2020), "Building Information Modelling : Evaluating Tools for Maturity and Benefits Measurement", No. February, p. 184.

Kassem, M., Succar, B., Dawood, N., Sher, W., Williams, A. and Kassem, M. (2013), "BIM in Practice: BIM Education", *Automation in Construction*.

Kayworth, T. and Whitten, D. (2010), "Effective information security requires a balance of social and technology factors", *MIS Quarterly Executive*.

Keady, R.A. (2013), "Financial Impact and analysis of equipment inventories", *Facilities Engineering Journal*.

Kelly, G., Serginson, M., Lockley, S., Dawood, N. and Kassem, M. (2013a), "BIM for

facility management: a review and a case study investigating the value and challenges", *Proceedings of the 13th International Conference on Construction Applications of Virtual Reality*, No. October, pp. 30–31.

Kelly, G., Serginson, M., Lockley, S., Dawood, N. and Kassem, M. (2013b), "103.Convr-2013-20", *13th International Conference Applications of Virtual Reality*.

Kennett, M., Letvin, E., Chipley, M. and Ryan, T. (2005), "FEMA 452-Risk Assessment", *Federal Emergency Management Agency*, No. January.

Kensek, K. (2015), "BIM guidelines inform facilities management databases: A Case Study over Time", *Buildings*, Vol. 5 No. 3, pp. 899–916.

Kensek, K.M. (2014), *Building Information Modeling*, *Building Information Modeling*, available at:https://doi.org/10.4324/9781315797076.

Khajuria, S., Sørensen, L. and Skouby, K.E. (2017), *Cybersecurity and Privacy - Bridging the Gap.*, *Cybersecurity and Privacy*.

Khorrami, F., Krishnamurthy, P. and Karri, R. (2016), "Cybersecurity for Control Systems: A Process-Aware Perspective", *IEEE Design and Test*, available at:https://doi.org/10.1109/MDAT.2016.2594178.

Khoshgoftar, M. and Osman, O. (2009), "Comparison of maturity models", *Proceedings - 2009 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009*, available at:https://doi.org/10.1109/ICCSIT.2009.5234402.

Khosrowshahi, F. and Arayici, Y. (2012), "Roadmap for implementation of BIM in the UK construction industry", *Engineering, Construction and Architectural Management*, available at:https://doi.org/10.1108/09699981211277531.

Kim, H., Anderson, K., Lee, S. and Hildreth, J. (2013), "Generating construction schedules through automatic data extraction using open BIM (building information modeling) technology", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2013.05.020.

Kitchin, D. and Kitchin, D. (2018), "Organisational Structures", *An Introduction to Organisational Behaviour for Managers and Engineers*, available at:https://doi.org/10.4324/9781315562933-8.

Knox, S. and Burkard, A.W. (2009), “Qualitative research interviews”, *Psychotherapy Research*, available at:https://doi.org/10.1080/10503300802702105.

Kopp, E., Kaffenberger, L. and Wilson, C. (2017), “Cyber Risk, Market Failures, and Financial Stability”, INTERNATIONAL MONETARY FUND, USA, available at:https://doi.org/https://doi.org/10.5089/9781484313787.001.

Kosseff, J. (2018), “Defining cybersecurity law”, *Iowa Law Review*.

Kothari, C. (2004), *Research Methodology: Methods and Techniques, New Age International*, available at:https://doi.org/http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf.

Kumar, M., Meena, J., Singh, R. and Vardhan, M. (2016), “Data outsourcing: A threat to confidentiality, integrity, and availability”, *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, available at:https://doi.org/10.1109/ICGCIoT.2015.7380703.

Kuo, R.Z. and Lee, G.G. (2011), “Knowledge management system adoption: Exploring the effects of empowering leadership, task-technology fit and compatibility”, *Behaviour and Information Technology*, available at:https://doi.org/10.1080/0144929X.2010.516018.

Kure, H.I., Islam, S. and Razzaque, M.A. (2018), “An integrated cyber security risk management approach for a cyber-physical system”, *Applied Sciences (Switzerland)*, available at:https://doi.org/10.3390/app8060898.

Kvale, S. (2011a), *Doing Interviews*, *Doing Interviews*, available at:https://doi.org/10.4135/9781849208963.

Kvale, S. (2011b), “Ethical Issues of Interviewing”, *Doing Interviews*, available at:https://doi.org/10.4135/9781849208963.n3.

Lacey, D. (2010), “Understanding and transforming organizational security culture”, *Information Management & Computer Security*, available at:https://doi.org/10.1108/09685221011035223.

Lagazio, M., Sherif, N. and Cushman, M. (2014), “A multi-level approach to understanding the impact of cyber crime on the financial sector”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2014.05.006.

Lam, J. (2017), *Implementing Enterprise Risk Management*, *Implementing Enterprise Risk Management*, available at:https://doi.org/10.1002/9781118922415.

Latiffi, A.A., Brahim, J., Mohd, S. and Fathi, M.S. (2015), "Building Information Modeling (BIM): Exploring Level of Development (LOD) in Construction Projects", *Applied Mechanics and Materials*, available at:https://doi.org/10.4028/www.scientific.net/amm.773-774.933.

Lavy, S. and Jawadekar, S. (2014), "A Case Study of Using BIM and COBie for Facility Management", *International Journal of Facility Management*.

Leavy, P. (2017), *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*, *BMC Public Health*.

Lee, J., Jeong, Y., Oh, Y.S., Lee, J.C., Ahn, N., Lee, J. and Yoon, S.H. (2013), "An integrated approach to intelligent urban facilities management for real-time emergency response", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2012.11.008.

Lee, Y.C., Eastman, C.M. and Solihin, W. (2018), "Logic for ensuring the data exchange integrity of building information models", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2017.08.010.

Lee, Y.C., Eastman, C.M., Solihin, W. and See, R. (2016), "Modularized rule-based validation of a BIM model pertaining to model views", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2015.11.006.

Leidner, D.E., Lo, J. and Preston, D. (2011), "An empirical investigation of the relationship of IS strategy with firm performance", *Journal of Strategic Information Systems*, available at:https://doi.org/10.1016/j.jsis.2011.09.001.

Leite, F., Akcamete, A., Akinci, B., Atasoy, G. and Kiziltas, S. (2011), "Analysis of modeling effort and impact of different levels of detail in building information models", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2010.11.027.

Lesk, M. (2011), "Cybersecurity and economics", *IEEE Security and Privacy*, available at:https://doi.org/10.1109/MSP.2011.160.

Leung, M.Y., Lu, X. and ip, H.Y. (2005), "Investigating key components of the facility management of secondary schools in Hong Kong", *Facilities*, available at:https://doi.org/10.1108/02632770510588637.

Leviton, L.C. (2015), “External Validity”, *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, available at:https://doi.org/10.1016/B978-0-08-097086-8.44025-0.

Lewis-Beck, M., Bryman, A. and Futing Liao, T. (2012), “Interviewing in Qualitative Research”, *The SAGE Encyclopedia of Social Science Research Methods*, available at:https://doi.org/10.4135/9781412950589.n455.

Li, X., Wu, C., Xu, B. and Mao, C. (2017), *Overview of BIM Maturity Measurement Tools*, *Journal of Information Technology in Construction (ITcon)*, Vol. 22, available at: http://www.itcon.org/2017/3 (accessed 24 January 2021).

Lin, Y.C., Chen, Y.P., Huang, W.T. and Hong, C.C. (2016), “Development of BIM execution plan for BIM model management during the pre-operation phase: A case study”, *Buildings*, available at:https://doi.org/10.3390/buildings6010008.

Lin, Y.C. and Su, Y.C. (2013), “Developing mobile- and BIM-based integrated visual facility maintenance management system”, *The Scientific World Journal*, available at:https://doi.org/10.1155/2013/124249.

Linderoth, H.C.J. (2010), “Understanding adoption and use of BIM as the creation of actor networks”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2009.09.003.

Liu, Z.Q., Li, Y.G. and Lu, X.L. (2009), “Development of Integrated Information Technology in the Chinese Building Industry”, *Proceedings of Shanghai International Conference on Technology of Architecture and Structure, Pt Ii*, pp. 544–553.

Liu, D., Wang, X. and Camp, L.J. (2009), “Mitigating inadvertent insider threats with incentives”, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, available at:https://doi.org/10.1007/978-3-642-03549-4_1.

Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C.L.P. (2012), “Cyber security and privacy issues in smart grids”, *IEEE Communications Surveys and Tutorials*, available at:https://doi.org/10.1109/SURV.2011.122111.00145.

Liu, Z., Chen, K., Peh, L. and Tan, K.W. (2017), “A feasibility study of Building Information Modeling for Green Mark New Non-Residential Building (NRB): 2015 analysis”,

Energy Procedia, available at:https://doi.org/10.1016/j.egypro.2017.12.651.

Lockamy, A. and McCormack, K. (2004), "Linking SCOR planning practices to supply chain performance: An exploratory study", *International Journal of Operations and Production Management*, available at:https://doi.org/10.1108/01443570410569010.

Lorimer, J. (2011), "Why do we need BIM? | NBS", 1 April, available at: https://www.thenbs.com/knowledge/why-do-we-need-bim (accessed 23 April 2021).

Louis, J. and Dunston, P.S. (2018), "Integrating IoT into operational workflows for real-time and automated decision-making in repetitive construction operations", *Automation in Construction*, Elsevier B.V., Vol. 94, pp. 317–327.

Love, P.E.D., Matthews, J., Simpson, I., Hill, A. and Olatunji, O.A. (2014), "A benefits realization management building information modeling framework for asset owners", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2013.09.007.

Loza de Siles, E. (2015), "Cybersecurity and Cybercrime: Intellectual Property and Innovation", *SSRN Electronic Journal*, available at:https://doi.org/10.2139/ssrn.2644365.

Maglaras, L.A., Kim, K.-H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., Maglaras, A., *et al.* (2018), "Cyber security of critical infrastructures", *ICT Express*, Elsevier BV, Vol. 4 No. 1, pp. 42–45.

Malatji, M., Marnewick, A. and von Solms, S. (2020), "Validation of a socio-technical management process for optimising cybersecurity practices", *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2020.101846.

Malatji, M., Von Solms, S. and Marnewick, A. (2019), "Socio-technical systems cybersecurity framework", *Information and Computer Security*, available at:https://doi.org/10.1108/ICS-03-2018-0031.

Mandani, A. and Ramirez, R. (2019), "Cybersecurity: Current state of governance literature", *25th Americas Conference on Information Systems, AMCIS 2019*.

Mankins, M.C. and Steele, R. (2005), "Turning great strategy into great performance", *Harvard Business Review*.

Mantha, B., de Soto, B. G., & Karri, R. (2020), "Cyber Security Threat Modeling in the

Construction Industry: A Countermeasure Example During the Commissioning Process", *The Open Archive of Engineering*, available at:https://doi.org/10.31224/osf.io/gn78a.

Mantha, B., García de Soto, B. and Karri, R. (2020), "Cyber Security Threat Modeling in the Construction Industry: A Countermeasure Example During the Commissioning Process", pp. 1–27.

Mantha, B.R.K. and de Soto, B.G. (2019), "Cyber security challenges and vulnerability assessment in the construction industry", available at:https://doi.org/10.3311/ccc2019-005.

Maradza, E., Whyte, J. and Larsen, G.D. (2013), "Standardisation of building information modelling in the UK and USA: Challenges and opportunities", *AEI 2013: Building Solutions for Architectural Engineering - Proceedings of the 2013 Architectural Engineering National Conference*, available at:https://doi.org/10.1061/9780784412909.044.

Marmo, R., Nicolella, M., Polverino, F. and Tibaut, A. (2019), "A methodology for a performance information model to support facility management", *Sustainability (Switzerland)*, Vol. 11 No. 24, pp. 1–25.

Martins, E.C. and Terblanche, F. (2003), "Building organisational culture that stimulates creativity and innovation", *European Journal of Innovation Management*, available at:https://doi.org/10.1108/14601060310456337.

Matarneh, S.T., Danso-Amoako, M., Al-Bizri, S., Gaterell, M. and Matarneh, R. (2019), "Building information modeling for facilities management: A literature review and future research directions", *Journal of Building Engineering*, available at:https://doi.org/10.1016/j.jobe.2019.100755.

Maxwell, J.A. (2013), "Conceptual Framework: What do you think is going on?", *Qualitative Research Design: An Interactive Approach*.

Mayo, G. and Snider, D. (2016), "Bas and cyber security: A multiple discipline perspective", *2016 International Annual Conference of the American Society for Engineering Management, ASEM 2016*.

McArthur, J.J. (2015), "A Building Information Management (BIM) Framework and

Supporting Case Study for Existing Building Operations, Maintenance and Sustainability", *Procedia Engineering*, Elsevier B.V., Vol. 118, pp. 1104–1111.

McCormack, K., Ladeira, M.B. and Valadares De Oliveira, M.P. (2008), "Supply chain maturity and performance in Brazil", *Supply Chain Management*, available at:https://doi.org/10.1108/13598540810882161.

McCuen, T.L., Suermann, P.C. and Krogulecki, M.J. (2012), "Evaluating Award-Winning BIM Projects Using the National Building Information Model Standard Capability Maturity Model", *Journal of Management in Engineering*, available at:https://doi.org/10.1061/(asce)me.1943-5479.0000062.

McGhee, G., Marland, G.R. and Atkinson, J. (2007), "Grounded theory research: Literature reviewing and reflexivity", *Journal of Advanced Nursing*, available at:https://doi.org/10.1111/j.1365-2648.2007.04436.x.

McGill, A. (2018), "Reporting with purpose and impact", *Pwc*.

McGraw Hill Construction. (2012), *The Business Value of BIM in North America, SmartMarket Report*.

McPhee, C. and Khan, O. (2015), "Editorial: Cyber-Resilience in Supply Chains (April 2015)", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 3–5.

Mell, P. and Grance, T. (2011), "The NIST definition of cloud computing - SP 800-145", *NIST Special Publication*.

Mellado, D., Blanco, C., Sánchez, L.E. and Fernández-Medina, E. (2010), "A systematic review of security requirements engineering", *Computer Standards & Interfaces*, Elsevier, Vol. 32 No. 4, pp. 153–165.

Merriam, S.B. (2009), *Qualitative Research: A Guide to Design and Implementation, The JosseyBass Higher and Adult Education Series*, available at:https://doi.org/10.1097/NCI.0b013e3181edd9b1.

Min, K.-S., Chai, S.-W. and Han, M. (2015), "An International Comparative Study on Cyber Security Strategy", *International Journal of Security and Its Applications*, NADIA, Vol. 9 No. 2, pp. 13–20.

Mingers, J. (2004), "Real-izing information systems: critical realism as an underpinning

philosophy for information systems", *Information and Organization*, Elsevier, Vol. 14 No. 2, pp. 87–103.

Mingers, J., Mutch, A. and Willcocks, L. (2013), "Critical Realism : Basic Concepts", *MIS Quarterly: Management Information Systems*.

Minoli, D., Sohraby, K. and Occhiogrosso, B. (2017), "IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems", *IEEE Internet of Things Journal*, available at:https://doi.org/10.1109/JIOT.2017.2647881.

Mohan, V., Ben Othmane, L. and Kres, A. (2018), "BP: Security concerns and best practices for automation of software deployment processes: An industrial case study", *Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev 2018*, available at:https://doi.org/10.1109/SecDev.2018.00011.

Mohanta, A. and Das, S. (2016), "ICT-Based facilities management tools for buildings", *Advances in Intelligent Systems and Computing*, available at:https://doi.org/10.1007/978-981-10-0129-1_14.

Mom, M. and Hsieh, S. (2012), "Toward performance assessment of BIM technology implementation", *14th International Conference on Computing in Civil and Building Engineering, 27-29 June*.

Morlhon, R., Pellerin, R. and Bourgault, M. (2015), "Defining building information modeling implementation activities based on capability maturity evaluation: A theoretical model", *International Journal of Information Systems and Project Management*, available at:https://doi.org/10.12821/ijispm030103.

MS/2 British Standards Institution. (2010), "BS 6079-1:2010 - Project management: Principles and guidelines for the management of projects", *<germanTitle/>*.

Mutis, I. and Paramashivam, A. (2019), "Cybersecurity Management Framework for a Cloud-Based BIM Model", *Advances in Informatics and Computing in Civil and Construction Engineering*, available at:https://doi.org/10.1007/978-3-030-00220-6_39.

Myers, M.D., Straub, D., Mingers, J. and Walsham, G. (2004), "The Great Quantitative/Qualitative Debate: The Past, Present, and Future of Positivism and Post-Positivism in Information Systems", *Information Systems Research*, Springer, pp. 659–

660.

Naghshbandi, S.N. (2016a), “BIM for Facility Management: Challenges and Research Gaps”, *Civil Engineering Journal*, available at:https://doi.org/10.28991/cej-2016-00000067.

Naghshbandi, S.N. (2016b), “BIM for Facility Management: Challenges and Research Gaps”, *Civil Engineering Journal*, Vol. 2 No. 12, pp. 679–684.

Nazir, S., Patel, S. and Patel, D. (2017), “Assessing and augmenting SCADA cyber security: A survey of techniques”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2017.06.010.

NCSC. (2018), “GUIDANCE 10 steps to cyber security”, *Ncsc.Gov.Uk*.

Nepal, M.P., Jupp, J.R. and Aibinu, A.A. (2014), “Evaluations of BIM: Frameworks and perspectives”, *Computing in Civil and Building Engineering - Proceedings of the 2014 International Conference on Computing in Civil and Building Engineering*, available at:https://doi.org/10.1061/9780784413616.096.

New BIM Standards - ISO19650. (2020), “Building Information Modelling, Digital information management to improve infrastructure delivery and performance”, available at: https://bimportal.scottishfuturestrust.org.uk/page/new-international-bim-standards.

Newswire, P.R. (2020), “The Future of Facility Management (FM), Forecast to 2025”, *Reportlinker-Facility*.

NIBS. (2015), “National BIM Standard - United States”, *National BIM Standard - United States - Version 3*.

NIBS. (2017), “National BIM Guide for Owners”, *NIBS*.

Nilsen, M. and Bohne, R.A. (2019), “Evaluation of BIM based LCA in early design phase (low LOD) of buildings”, *IOP Conference Series: Earth and Environmental Science*, available at:https://doi.org/10.1088/1755-1315/323/1/012119.

NIMBS Committe. (2007), “National Building Information Modeling Standard”, *Nbim*.

NIST. (2003), *Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50*.

NIST. (2013), *Glossary of Key Information Security Terms, NIST IR*.

NIST. (2020a), “Integrating Cybersecurity and Enterprise Risk Management (ERM): Second Public Draft of NISTIR 8286”, available at: https://www.nist.gov/news-events/news/2020/07/integrating-cybersecurity-and-enterprise-risk-management-erm-second-public (accessed 21 September 2020).

NIST. (2020b), *Integrating Cybersecurity and Enterprise Risk Management (ERM)*.

Noble, H. and Smith, J. (2015), “Issues of validity and reliability in qualitative research”, *Evidence-Based Nursing*, available at:https://doi.org/10.1136/eb-2015-102054.

Nokhbeh Zaeem, R., Manoharan, M., Yang, Y. and Barber, K.S. (2017), “Modeling and analysis of identity threat behaviors through text mining of identity theft stories”, *Computers and Security*, Elsevier Ltd, Vol. 65, pp. 50–63.

Nye, J. (2018), “How Will New Cybersecurity Norms Develop?”, *Project Syndicate*.

O’Leary, Z. (2021), *The Essential Guide to Doing Your Research Project*, Sage.

O’Neil, C. and Saleeb, D.N. (2019), “ Organisational Information Requirements for Successful BIM Implementation ”, *Global Construction Success*, available at:https://doi.org/10.1002/9781119440345.ch22.

Olivier, M.S. (2002), “Database Privacy: Balancing Confidentiality, Integrity and Availability”, *SIGKDD Explorations*.

Onwuegbuzie, A.J., Leech, N.L. and Collins, K.M.T. (2012), “Qualitative analysis techniques for the review of the literature”, *Qualitative Report*.

Owen, G.T. (2014), “Qualitative methods in higher education policy analysis: Using interviews and document analysis”, *The Qualitative Report*, The Qualitative Report, Vol. 19 No. 26, p. 1.

Oxtoby, B., McGuiness, T. and Morgan, R. (2002), “Developing organisational change capability”, *European Management Journal*, available at:https://doi.org/10.1016/S0263-2373(02)00047-6.

Parn, E.A. and Edwards, D. (2019), “Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence”, *Engineering, Construction and Architectural Management*, available at:https://doi.org/10.1108/ECAM-03-2018-0101.

Pärn, E.A., Edwards, D.J. and Sing, M.C.P. (2017), "The building information modelling trajectory in facilities management: A review", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2016.12.003.

Patacas, J., Dawood, N., Greenwood, D. and Kassem, M. (2016), "Supporting building owners and facility managers in the validation and visualisation of asset information models (aim) through open standards and open technologies", *Journal of Information Technology in Construction*, Vol. 21 No. January, pp. 434–455.

Patacas, J., Dawood, N., Vukovic, V. and Kassem, M. (2015), "BIM for facilities management: Evaluating BIM standards in asset register creation and service life planning", *Journal of Information Technology in Construction*, Vol. 20 No. August, pp. 313–331.

Paulk, M.C. (1995), "How ISO 9001 Compares with the CMM", *IEEE Software*, available at:https://doi.org/10.1109/52.363163.

Paulsen, C. Toth, P. (2016), "Small Business Information Security: The Fundamentals Small Business", *National Institute of Standards and Technology Interagency Report*.

Pawlowski, Suzanne D, Okoli, C. (2004), "The Delphi Method as a Research Tool : An Example , Design Considerations and Applications 1 Introduction 2 Overview of the Delphi method", *Information & Management*.

Peansupap, V. and Walker, D.H.T. (2005), "Factors enabling information and communication technology diffusion and actual implementation in construction organisations", *Electronic Journal of Information Technology in Construction*.

Pishdad-Bozorgi, P., Gao, X., Eastman, C. and Self, A.P. (2018), "Planning and developing facility management-enabled building information model (FM-enabled BIM)", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2017.12.004.

Pohontsch, N.J. (2019), "Qualitative Content Analysis", *Rehabilitation (Germany)*, available at:https://doi.org/10.1055/a-0801-5465.

Portal, B. (2020), "Determine the Info Management & CDE Strategy Common Data Environment (CDE) Strategy", available at: https://bimportal.scottishfuturestrust.org.uk/level2/stage/1/task/22/overview-of-the-common-data-environment-cde (accessed 1 September 2020).

Posthumus, S. and Von Solms, R. (2004), “A framework for the governance of information security”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2004.10.006.

Pratt, M.J. (2001), “Introduction to iso 10303—the step standard for product data exchange”, *Journal of Computing and Information Science in Engineering*, available at:https://doi.org/10.1115/1.1354995.

“Project Phases & Level of Development | Insight | Autodesk Knowledge Network”. (n.d.). *2017*, available at: https://knowledge.autodesk.com/support/insight/learn-explore/caas/simplecontent/content/project-phases-level-development.html (accessed 5 December 2020).

Puolitaival, T. and Forsythe, P. (2016), “Practical challenges of BIM education”, *Structural Survey*, available at:https://doi.org/10.1108/SS-12-2015-0053.

Purpura, P.P. (2019), “Critical Infrastructure Protection and Cybersecurity”, *Security and Loss Prevention*, available at:https://doi.org/10.1016/b978-0-12-811795-8.00016-3.

Qu, S.Q. and Dumay, J. (2011), “The qualitative research interview”, *Qualitative Research in Accounting & Management*, Emerald Group Publishing Limited.

Radl, J. and Kaiser, J. (2019), “Benefits of Implementation of Common Data Environment (CDE) into Construction Projects”, *IOP Conference Series: Materials Science and Engineering*, available at:https://doi.org/10.1088/1757-899X/471/2/022021.

Requirements, F. (n.d.). “UK Government BIM Working Group CDE Sub Group Asset Information Management - Common Data Environment”.

RIBA. (2012), *BIM Overlay to the RIBA Outline Plan of Work, Royal Institute of British Architects*.

Richard, M. (2018), “BIM Levels explained | NBS”, *Nbs*.

Richardson, R., and North, M.M. (2017), “Ransomware: Evolution, mitigation and prevention”, *International Management Review*, Vol. 13 No. 1, p. 10.

RICS. (2017), “Building Information Modelling for Project Managers”, *Bim-Pm*.

RICS. (2018), *Strategic Facility Management Framework RICS Guidance Note*, London.

Rivera, J. (2017), “Cyber security via formal methods: A framework for implementing formal

methods", *2017 IEEE International Conference on Cyber Conflict U.S., CyCon U.S. 2017 - Proceedings*, available at:https://doi.org/10.1109/CYCONUS.2017.8167500.

Rowe, N. and Garfinkel, S. (2012), "Finding suspicious activity on computer systems", *11th European Conference on Information Warfare and Security 2012, ECIW 2012*.

Royer, I. and Zarlowski, P. (2001), "Doing Management Research", SAGE Publications Ltd, London, available at:https://doi.org/10.4135/9781849208970.

Rudestam, K.E. and Newton, R.R. (2014), "Surviving your dissertation: A comprehensive guide to content and process", Sage Publications.

De Sá, A.O., Carmo, L.F.R.D.C. and Machado, R.C.S. (2017), "Covert Attacks in Cyber-Physical Control Systems", *IEEE Transactions on Industrial Informatics*, available at:https://doi.org/10.1109/TII.2017.2676005.

Sackey, E., Tuuli, M.M. and Dainty, A. (2013), "Bim Implementation : From Capability Maturity Models To Implementation Strategy", *Sustainable Building Conference 2013*.

Sacks, R., Eastman, C., Lee, G. and Teicholz, P. (2018), *A Guide to Building Information Modeling for Owners, Designers, Engineers, Contractors, and Facility Managers*.

Sacks, R., Gurevich, U. and Shrestha, P. (2016a), "A review of Building Information Modeling protocols, guides and standards for Large construction clients", *Journal of Information Technology in Construction*.

Sacks, R., Gurevich, U. and Shrestha, P. (2016b), "A review of Building Information Modeling protocols, guides and standards for Large construction clients", *Journal of Information Technology in Construction*, Vol. 21 No. January 2017, pp. 479–503.

Saleh, M.S. and Alfantookh, A. (2011), "A new comprehensive framework for enterprise information security risk management", *Applied Computing and Informatics*, available at:https://doi.org/10.1016/j.aci.2011.05.002.

Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B. (2019), "Strategy and organisational cybersecurity: a knowledge-problem perspective", *Journal of Intellectual Capital*, available at:https://doi.org/10.1108/JIC-03-2019-0041.

Salminen, M. (2019), "Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North", *The Yearbook of Polar Law Online*, available

at:https://doi.org/10.1163/22116427_010010015.

Sandelowski, M. (1998), “Focus on Qualitative Methods the Call to Experts in Qualitative Research”, *Research in Nursing and Health*, available at:https://doi.org/10.1002/(sici)1098-240x(199810)21:5<467::aid-nur9>3.0.co;2-l.

Sapsford, R. and Jupp, V. (2012), *Data Collection and Analysis*, *Data Collection and Analysis*, available at:https://doi.org/10.4135/9781849208802.

Sapsford, R., Jupp, V., Abbott, P. and Sapsford, R. (2012), “Ethics, Politics and Research”, *Data Collection and Analysis*, available at:https://doi.org/10.4135/9781849208802.n13.

Saunders, M., Lewis, P. and Thornhill, A. (2019), *Chapter 4: Understanding Research Philosophy and Approaches to Theory Development*, *Research Methods for Business Students*.

Sayer, A. (2000), *Introducing Critical Realism*, *Realism and Social Science*.

Schade, J., Olofsson, T. and Schreyer, M. (2011), “Decision-making in a model-based design process”, *Construction Management and Economics*, available at:https://doi.org/10.1080/01446193.2011.552510.

Schumacher, A., Erol, S. and Sihn, W. (2016), “A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises”, *Procedia CIRP*, available at:https://doi.org/10.1016/j.procir.2016.07.040.

Scovetta, V. (2013), *The Impact of Leadership Social Power on Knowledge Management Success*, *ProQuest Dissertations and Theses*.

Scully, T. (2011), “The cyber threat, trophy information and the fortress mentality.”, *Journal of Business Continuity & Emergency Planning*.

Scully, T. (2013), “The cyber security threat stops in the boardroom.”, *Journal of Business Continuity & Emergency Planning*.

Sebastian, R. and Van Berlo, L. (2010), “Tool for benchmarking BIM performance of design, engineering and construction firms in the Netherlands”, *Architectural Engineering and Design Management*, available at:https://doi.org/10.3763/aedm.2010.IDDS3.

SEI. (2010), *CMMI® for Development, Version 1.3 CMMI-DEV, V1.3 - Improving Processes for Developing Better Products and Services*, *Engineering*.

"SEI Capability Maturity Model's impact on Contractors". (1995), *Computer*, available at:https://doi.org/10.1109/2.362633.

Sekaran, U. and Bougie, R. (2016), *Research Methods for Business: A Skill Building Approach*, John Wiley & Sons.

Selamat, M.H. and Ibrahim, O. (2018), "The Moderating Effect of Risk Culture in Relationship between Leadership and Enterprise Risk Management Implementation in Malaysia", *Culture*, Vol. 9 No. 1.

Services, A.W. (2018), "Types of Cloud Computing", available at: https://aws.amazon.com/types-of-cloud-computing/.

Shad, M.K., Lai, F.W., Fatt, C.L., Klemeš, J.J. and Bokhari, A. (2019), "Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework", *Journal of Cleaner Production*, available at:https://doi.org/10.1016/j.jclepro.2018.10.120.

Sherman, A.T., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., Herman, G.L., *et al.* (2017), "Cybersecurity: Exploring core concepts through six scenarios", *Cryptologia*, available at:https://doi.org/10.1080/01611194.2017.1362063.

Shiem Shin Then, D. (1999), "An integrated resource management view of facilities management", *Facilities*, available at:https://doi.org/10.1108/02632779910293451.

Shillcock, P. (2019), "From BS 1192 to ISO 19650 and everything in between", *NBS*.

Sinclair, D. (2019), *Assembling a Collaborative Project Team: Practical Tools Including Multidisciplinary Schedules of Services*, Routledge.

Siponen, M. and Willison, R. (2009), "Information security management standards: Problems and solutions", *Information & Management*, Elsevier BV, Vol. 46 No. 5, pp. 267–270.

Slagmulder, R. and Devoldere, B. (2018), "Transforming under deep uncertainty: A strategic perspective on risk management", *Business Horizons*, available at:https://doi.org/10.1016/j.bushor.2018.05.001.

Smith, C.L. and Brooks, D.J. (2013), "Concept of Security", *Security Science*, available at:https://doi.org/10.1016/b978-0-12-394436-8.00001-1.

Smith, D. and Figp, H. (2010), *Architecture, Engineering, Construction, Owner Operator*

Phase 1 (AECOO-1) Joint Testbed.

Smith, P. (2014), "BIM implementation - Global strategies", *Procedia Engineering*, available at:https://doi.org/10.1016/j.proeng.2014.10.575.

Snyder, H. (2019), "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, available at:https://doi.org/10.1016/j.jbusres.2019.07.039.

von Solms, B. and von Solms, R. (2018), "Cybersecurity and information security – what goes where?", *Information and Computer Security*, available at:https://doi.org/10.1108/ICS-04-2017-0025.

Von Solms, R. and Van Niekerk, J. (2013), "From information security to cyber security", *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2013.04.004.

Sommer, P. and Brown, I. (2011), "Reducing systemic cyber security risk", *Organisation for Economic Cooperation and Development Working Paper*.

Song, S., Kim, B. and Lee, S. (2016), "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", *Mobile Information Systems*, available at:https://doi.org/10.1155/2016/2946735.

Sophos. (2014), "Internet Security Threat Report , SOPHOS", *Security*.

Srinivas, J., Das, A.K. and Kumar, N. (2019), "Government regulations in cyber security: Framework, standards and recommendations", *Future Generation Computer Systems*, available at:https://doi.org/10.1016/j.future.2018.09.063.

Stallings, W. and Bauer, M. (2011), *Computer Security: Principles and Practice*, *Computer Fraud & Security Bulletin*.

Stanton, J.M., Mastrangelo, P.R., Stam, K.R. and Jolton, J. (2004), "Behavioral information security: two end usersurvey studies of motivation and security practices", *Behavioral Information Security*.

State of Ohio. (2010), *State of Ohio Building Information Modeling Protocol*, Ohio.

Steiner, J. (2006), "The art of space management: Planning flexible workspaces for people", *Journal of Facilities Management*, available at:https://doi.org/10.1108/14725960610644195.

Steward, B. (2004), “Writing a literature review”, *British Journal of Occupational Therapy*, available at:https://doi.org/10.1177/030802260406701105.

Stuckey, H. (2013), “Three types of interviews: Qualitative research methods in social health”, *Journal of Social Health and Diabetes*, available at:https://doi.org/10.4103/2321-0656.115294.

Succar, B. (2009), “Building information modelling framework: A research and delivery foundation for industry stakeholders”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2008.10.003.

Succar, B. (2010), “Building Information Modelling Maturity Matrix”, available at:https://doi.org/10.4018/978-1-60566-928-1.ch004.

Succar, B. (2015), “UK BIM maturity model”, available at: http://changeagents.blogs.com/thinkspace/ (accessed 10 April 2021).

Succar, B., Sher, W. and Williams, A. (2013), “An integrated approach to BIM competency assessment, acquisition and application”, *Automation in Construction*, Elsevier B.V., Vol. 35, pp. 174–189.

Sullivan, G.P., Pugh, R., Melendez, a P. and Hunt, W.D. (2010), *Operations & Maintenance Best Practices, Pacific Northwest National Laboratory for the Federal Energy Management Program U.S. Department of Energy*.

Supić, H. (2005), “Project management maturity of selected organizations in Croatia”, *Proceedings of the 8th International Conference on Telecommunications, ConTEL 2005*, available at:https://doi.org/10.1109/contel.2005.185978.

Tagarev, T. (2020), “Governance of Collaborative Networked Organisations: Stakeholder Requirements”, *Proceedings - 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies, DESSERT 2020*, available at:https://doi.org/10.1109/DESSERT50317.2020.9125029.

Tang, S., Shelden, D.R., Eastman, C.M., Pishdad-Bozorgi, P. and Gao, X. (2020), “BIM assisted Building Automation System information exchange using BACnet and IFC”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2019.103049.

Task Force Transformation Initiative, J. (2015), “NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations JOINT TASK

FORCE TRANSFORMATION INITIATIVE", *NIST Special Publication*.

Taylor, S. (2012), "Qualitative Researc h", *Qualitative Research*, Vol. 12 No. 4, pp. 388–401.

The BIM Hub. (2018), "Defining FM and Client Information: OIR, AIR, PLQ and EIR | Opinion | The BIM Hub", *Thebimhub.Com*.

The International Organization for Standardization. (2012), "ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity", *ISO.Org [Online]*.

Theiler, M. and Smarsly, K. (2018), "IFC Monitor – An IFC schema extension for modeling structural health monitoring systems", *Advanced Engineering Informatics*, available at:https://doi.org/10.1016/j.aei.2018.04.011.

Thomborson, C. (2010), "A framework for system security", *Handbook of Information and Communication Security*, Springer, pp. 3–20.

Thompson, A.A.J., Strickland, A.J.I. and Gamble, J.E. (2018), *Crafting & Executing Strategy*, *Sedv 623*.

Tookey, J.E., Kulatunga, K., Kulatunga, U., Amaratunga, D. and Haigh, R. (2011), "Client's championing characteristics that promote construction innovation", *Construction Innovation*, available at:https://doi.org/10.1108/14714171111175873.

Trochim, W.M.K. and Donnelly, J.P. (2001), *Research Methods Knowledge Base*, Vol. 2, Atomic Dog Pub.

Tropina, T. (2020), "Cybercrime: Setting international standards", *Routledge Handbook of International Cybersecurity*, available at:https://doi.org/10.4324/9781351038904-14.

Tsoutsos, N.G., Gupta, N. and Karri, R. (2020), "Cybersecurity Road Map for Digital Manufacturing", *Computer*, IEEE, Vol. 53 No. 9, pp. 80–84.

Tuptuk, N. and Hailes, S. (2018), "Security of smart manufacturing systems", *Journal of Manufacturing Systems*, Elsevier BV, Vol. 47, pp. 93–106.

UK BIM Framework. (2020), "UK BIM Framework – BIM Standards, Guides & Resources", *Https://Ukbimframework.Org/*.

"UK BIM Framework – BIM Standards, Guides & Resources". (2019), *Https://Www.Ukbimframework.Org/*.

Ula, M., Ismail, Z. and Sidek, Z. (2011), “A Framework for the Governance of Information Security in Banking System”, *Journal of Information Assurance & Cybersecurity*, available at:https://doi.org/10.5171/2011.726196.

Underwood, J. and Shelbourn, M. (2021), *Handbook of Research on Driving Transformational Change in the Digital Built Environment*.

Vaidyanathan, K. and Howell, G. (2007), “Construction supply chain maturity model - Conceptual framework”, *Lean Construction: A New Paradigm for Managing Capital Projects - 15th IGLC Conference*.

Valunaite Oleskeviciene, G. and Sliogeriene, J. (2020), “Research methodology”, *Numanities - Arts and Humanities in Progress*, available at:https://doi.org/10.1007/978-3-030-37727-4_2.

Da Veiga, A. and Eloff, J.H.P. (2007), “An information security governance framework”, *Information Systems Management*, available at:https://doi.org/10.1080/10580530701586136.

Da Veiga, A. and Eloff, J.H.P. (2010), “A framework and assessment instrument for information security culture”, *Computers and Security*, available at:https://doi.org/10.1016/j.cose.2009.09.002.

Vishwakarma, A. (2016), “Virtual private networks”, *Network Security Attacks and Countermeasures*, available at:https://doi.org/10.4018/978-1-4666-8761-5.ch003.

Volk, R., Stengel, J. and Schultmann, F. (2014), “Building Information Modeling (BIM) for existing buildings - Literature review and future needs”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2013.10.023.

Wamala, F. (2011), *ITU National Cybersecurity Strategy Guide*, *Chemistry & …*.

Wang, B., Li, H., Rezgui, Y., Bradley, A. and Ong, H.N. (2014), “BIM based virtual environment for fire emergency evacuation”, *Scientific World Journal*, available at:https://doi.org/10.1155/2014/589016.

Wang, D., Abdelzaher, T. and Kaplan, L. (2015), *Social Sensing: Building Reliable Systems on Unreliable Data*, *Social Sensing: Building Reliable Systems on Unreliable Data*, available at:https://doi.org/10.1016/C2013-0-18808-3.

Wang, Y., Wang, X., Wang, J., Yung, P. and Jun, G. (2013), "Engagement of facilities management in design stage through BIM: Framework and a case study", *Advances in Civil Engineering*, available at:https://doi.org/10.1155/2013/189105.

Whitman, M.E. and Mattord, H.J. (2012), "Implementing Information Security", *Principles of Information Security*.

Wiles, R., Crow, G., Heath, S. and Charles, V. (2008), "The management of confidentiality and anonymity in social research", *International Journal of Social Research Methodology*, available at:https://doi.org/10.1080/13645570701622231.

Winzar, H., Baumann, C. and Chu, W. (2018), "Brand competitiveness", *International Journal of Contemporary Hospitality Management*, available at:https://doi.org/10.1108/ijchm-11-2016-0619.

Woiceshyn, J. and Daellenbach, U. (2018), "Evaluating inductive vs deductive research in management studies", *Qualitative Research in Organizations and Management: An International Journal*, available at:https://doi.org/10.1108/qrom-06-2017-1538.

Wong, C.H., Holt, G.D. and Cooper, P.A. (2000), "Lowest price or value? Investigation of UK construction clients' tender selection process", *Construction Management and Economics*, Taylor & Francis, Vol. 18 No. 7, pp. 767–774.

Wood, B. (2000), "An insider threat model for adversary simulation", *SRI International Research on Mitigating the Insider Threat to Information Systems*.

Wood, M.D., Wells, E.M., Rice, G. and Linkov, I. (2019), "Quantifying and mapping resilience within large organizations", *Omega (United Kingdom)*, available at:https://doi.org/10.1016/j.omega.2018.08.012.

Woods, M. (2011), "Interviewing for research and analysing qualitative data : An overview", *School of Humanities and Social Sciences, Massey University*.

Wu, C., Xu, B., Mao, C. and Li, X. (2017), "Overview of bim maturity measurement tools", *Journal of Information Technology in Construction*.

Wu, W. and Issa, R.R.A. (2015), "BIM Execution Planning in Green Building Projects: LEED as a Use Case", *Journal of Management in Engineering*, available at:https://doi.org/10.1061/(asce)me.1943-5479.0000314.

Yam, R.C.M., Tse, P.W., Li, L. and Tu, P. (2001), “Intelligent predictive decision support system for condition-based maintenance”, *International Journal of Advanced Manufacturing Technology*, available at:https://doi.org/10.1007/s001700170173.

Yaqoob, I., Ahmed, E., Rehman, M.H. ur, Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M. (2017), “The rise of ransomware and emerging security challenges in the Internet of Things”, *Computer Networks*, available at:https://doi.org/10.1016/j.comnet.2017.09.003.

Yin, R.K. (2014), *Case Study Research: Design and Methods (5th Ed.), Thousand Oaks, CA: SAGE Publications*.

Yin, R.K. (2018), *Understanding Qualitative Research, Handbook of Qualitative Research*.

Zachariadis, M., Scott, S. and Barrett, M. (2013), “Methodological implications of critical realism for mixed-methods research”, *MIS Quarterly: Management Information Systems*, available at:https://doi.org/10.25300/misq/2013/37.3.09.

Zhang, J., Seet, B.C. and Lie, T.T. (2015), “Building information modelling for smart built environments”, *Buildings*, available at:https://doi.org/10.3390/buildings5010100.

Zhang, S., Sulankivi, K., Kiviniemi, M., Romo, I., Eastman, C.M. and Teizer, J. (2015), “BIM-based fall hazard identification and prevention in construction safety planning”, *Safety Science*, Elsevier BV, Vol. 72, pp. 31–45.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2020), “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study”, *Journal of Computer Information Systems*, available at:https://doi.org/10.1080/08874417.2020.1712269.

Publications

- Ghadiminia.N, Mayouf.M, Cox.S, Krasniewicz.J (2021) 'BIM-enabled Facilities Management (FM): A Scrutiny of Risks Resulting from Cyber Attacks', Journal of Facilities Management
- IoT Security Foundation. (2019), *Can You Trust Your Smart Building?, IoT Security Foundation*.Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/06/IoTSF-Smart-Buildings-White-Paper-PDF-1.pdf

BIM-enabled Facilities Management (FM): A Scrutiny of Risks Resulting from Cyber Attacks

Nikdokht Ghadiminia and Mohammad Mayouf

School of Engineering and the Built Environment, Birmingham City University

Sharon Cox

School of Computing and Digital Technology, Birmingham City University

Jan Krasniewicz

School of Computing and Digital Technology, Birmingham City University

Abstract

Purpose – BIM creates a golden thread of information of the facility, which proves useful to those with malicious intents of breaching the security of the facility. A cyber-attack incurs adverse implications for the facility and its managing organisation. Hence, this paper aims to unravel the impact of a cybersecurity breach, by developing a BIM-FM cybersecurity-risk-matrix to portray what a cybersecurity-attack means for various working areas of FM.

Design/methodology/approach – This study commenced with exploring cybersecurity within various stages of a BIM project. This showcased a heightened risk of cybersecurity at the post-occupancy phase. Hence, thematic analysis of two main domains of BIM-FM and cybersecurity in the built environment led to the development of a matrix that illustrated the impact of a cybersecurity attack on a BIM-FM organisation.

Findings- Findings show that the existing approaches to the management of cybersecurity in BIM-FM are technology dependent, resulting in an over-reliance on technology and a lack of cybersecurity awareness of aspects related to people and process. This study sheds light on the criticality of cyber-risk at the post-occupancy phase, highlighting the FM areas which will be compromised as a result of a cyber-attack.

Originality/value – This study seeks to shift focus to the people and process aspects of cybersecurity in BIM-FM. Through discussing the interconnections between the physical and digital assets of a built facility, this study develops a cyber-risk matrix which acts as a foundation for empirical investigations of the matter in future research.

Keywords- BIM, FM, Cybersecurity, Risks, Threats, Cyber-awareness

Appendix 1. Interview Participation Form

Research Participation Agreement

Dear Participant,

I am a Doctoral Researcher at the school of Computing, Engineering and Built Environment at the Birmingham City University. I am investigating cybersecurity management in BIM-enabled Facilities Management. My specific interest is in the challenges brought by the interaction of people with digital technology offered by Building Information Modelling, and the ways in which the information will be exchanged and stored using various methods. The aim is to investigate the requirements improving the cybersecurity of BIM, for achieving its benefits within the facility management sector.

I would be most grateful if you would volunteer to assist in a study that I am conducting by granting an interview. No more than one hour would be required either face-to-face or via a call, depending on your availability and preference. This interview is for me to gain a better understanding of the issues affecting good cybersecurity culture within the FM sector with a focus on BIM-enabled projects and the knowledge and skills required to improve the security of digital data within FM. I will seek your consent before the interview starts as I intend to audio record the interview. Full anonymity and confidentiality are guaranteed for all participants that take part in this research and any work to be published as a result of this research will be done so in agreement with all parties.

This research project is designed and conducted by Nikdokht Ghadiminia, a PhD candidate at Birmingham City University.

Participation - Your participation in this interview is voluntary and you may withdraw your participation at any time. You understand that fully **anonymised** extracts from the interview may be quoted in the published PhD thesis.

Benefits - You will receive no direct benefits from participating in this research study. However, your responses will provide useful findings in the development of a practical framework used for improving the cybersecurity of the digital data (i.e., BIM data).

Risks - There are no foreseeable risks involved in participating in this study other than those encountered in day-to-day life.

Confidentiality - All your responses will remain anonymous without revealing personal details. All interview data are treated with utmost confidentiality in any publications or presentations and will remain anonymized.

Consent of Participation

I ----------(Name/Surname) here-by confirm that I am willing to participate in an interview on the information management strategies practiced by Facility Management stakeholders.

Your signature will also confirm the following:

- You have read the above information
- You understand that this interview will be audio recorded for researchers use only.
- You understand that all personal data will be kept strictly confidential.
- You voluntarily agree to participate
- You are 18 years of age or older

Please include your contact details to receive a copy of the framework developed from this research.

Telephone: ----------

Email: ----------

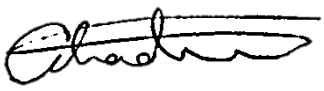
Researcher: Nikdokht Ghadiminia, BEng, MSc, PGCert,

Director of Studies: Dr Mohammad Mayouf, **PhD, MSc, PGCert, BSc, CAPM, FHEA, ACIOB**

Participant Signature: ----------

Date: ----------

Researcher Signature:



Date: ----------

Appendix 2. Validation Questionnaire Consent Form

Participation Agreement

Title of Research: An organizational approach to improving the cybersecurity of BIM-enabled facilities management.

Researcher: Nikdokht Ghadiminia, PhD Candidate, Birmingham City University

Aim of study: The aim of this research is to develop a framework that supports the integration of cyber security within the BIM-enabled facilities management organisations. This study explores the enablers and inhibitors of maintaining a cybersecure BIM-enabled facilities management by accentuating the role of people and processes.

Participant selection

You are selected as an expert with either facilities management or organisational cybersecurity management expertise to contribute to the validation of the framework proposed by this research. The validation task involves answering a questionnaire on the concepts within the framework. Your participation is voluntary, and you can withdraw at any point without justification. You will be asked to sign a consent form upon your participation.

Confidentiality: All responses and information collected from the questionnaire will be kept secure and no personally identifiable information will be kept or reported. All information will be managed in accordance with the Data Protection Act. The data collection process complies with the Birmingham city university's research code of conduct.

Withdrawal: You can withdraw your participation at any point. Also, you may inform the researcher if you do not wish any of your answers to be used in the research.

Description of the validation activity: As an expert with knowledge of facilities management and/or cybersecurity management, you are asked to respond to open ended questions regarding the proposed research framework. All participants will be given a research brief, which includes the research framework, a description of the framework and a table of description for the elements within the framework. You are asked to read the research brief prior to responding to the questionnaire. The questions are aimed at improving and optimising the proposed framework using your valuable insight. You are not obliged to answer to every question; however, every comment will add value to the research and is much appreciated.

Benefits: Participation in this research does not entail any financial gain for the participants. However, the facilities management industry will benefit from your valuable contribution to the development of a framework which can potentially guide them towards a cybersecure adoption and implementation of BIM.

Concerns:

No serious concerns are anticipated as a result of participation in study. However, you can always communicate your concerns to me or my director of studies if further details were required. Please find the contact details below:

- Researcher: Nikdokht Ghadiminia, Doctor of Philosophy Research Candidate, Birmingham City University, email: contact phone number:
- Director of Studies: Dr Mohammad Mayouf, Birmingham City University, Brunel email: Mohammad.Mayouf@bham.ac.uk

Participant's Signature:

Date:

Appendix 3. Interview Questions

Table 10- Interview Questions

No.	Questions	Focus
Q1	In which sector within the built environment does your organization operate?	Respondents' profile (excluded from coding)
Q2	What is your position within the organization?	
Q3	What is your experience with the facilities management? In which areas have you been involved?	
Q4	What is your perception of information security?	To understand respondent's perception of cybersecurity and BIM
Q5	What is your perception of BIM?	
Q6	In your opinion, what is taken into account when doing a BIM project? P1. Does it encompass any regulatory cybersecurity requirements for the exchange of BIM data? P2. Has your organization considered documenting cybersecurity objectives within the organizational mission statement? P3. What are the inhibitors/challenges of integrating cybersecurity in the FM BIM documentations?	To explore the driving/inhibiting attributes of integrating cyber security within BIM-enabled Facilities Management Organizations.
Q7	Do you have Risk Management Process maps for various areas of Facility management? Does it address cyber risks?	To understand how theory, practice, and regulation incorporate cybersecurity practices in the implementation of BIM-enabled FM.
Q8	Is your organization in compliance with any specific BIM standards for the exchange, archive, and access of BIM data? P1. Do the regulatory BIM requirements of your organization encompass cybersecurity regulatory requirements for the exchange, archive, and access of digital data?	

Q9	Has a managerial component/department of your organization been assigned to carry a duty of care/responsibility regarding the protection of BIM data against cyber-attacks? (Senior Cybersecurity Leadership) P1. Is cybersecurity incorporated into all FM employees (technical and non-technical staff) job descriptions? Or is one person or one department taking all the responsibility regarding the cybersecurity of all data?	
Q10	Has your organisation documented the organisational BIM capabilities related to Software, Hardware and Networking Systems facilitating BIM? P1. In your opinion, what are the challenges of maintaining trustworthiness in the aforementioned facilities in terms of their security? P2. Do you believe identifying the risk profile of such software through a risk assessment would be feasible?	
Q11	Does your organisation have a written document on the data exchange specifications? P1. Does it encompass any regulatory cybersecurity requirements for the exchange of BIM data? P2. In your opinion, how can your organization improve the security of data in the digital exchange processes? (Continuous process improvement)	
Q12	Does your organisation have a written document on the data requirements various FM areas and work tasks? (Asset management, Space management, Systems control & monitoring, and maintenance management) P1. In your opinion, do you believe that the development of a risk profile (source of potential threat, risk owner, vulnerabilities) for the FM digital data would lead to security aware decision making? P2. In your opinion, what are the main inhibitors of maintaining the security of data in various areas of facility management?	

Q.13	How does your organisation ensure the current policies of information management are effective? Does an evaluation of cybersecurity status take place within the benchmarking procedures?	To explore the social determinants cybersecurity within BIM-enabled Facilities Management.
Q.14	In your opinion, how can education and training programs contribute to a cybersecure culture within your organization?	

Appendix 4. Validation Questionnaire

No response required

Further explanation/clarification required

Response required

Table 11- Validation Responses

	BIMCS-FM	Questions	Feedback E1	Feedback E2	Feedback E3	Feedback E4	Feedback E5	Feedback E6	Feedback E7
BIMCS-FM Structure	Improving cybersecurity management of BIM-FM should be tackled from three aspects: Strategy Implementation Performance Hence, BIMCS-FM presents the determinants in three layers of strategy,	Q1. Having read the description of the terminologies within the layers of the framework, from your perspective, how familiar were you with these	Generally familiar with the terminology	These are understood, although they are not usually considered on smaller BIM projects which constitute the greater portion of my consultant support efforts.	Very familiar, I have been working on the aspects of standardization of these for some years, including roll-out at large FM practices.	I am familiar with these terminologies for general FM cyber security.	Yes, I was familiar	Yea, all the terminologies make sense. We haven't implemented any cyber security measures on projects, so my practical experience of the concepts put forward, would be limited.	Very. But don't focus just on cyber; BIM is a way of working that will involve physical documentation as well as electronic for some time.

	implementation, and performance.	terminologies?							
		Q2: (if yes: Does this framework trigger a change in your understanding of these concepts?)	Yes, my understanding was that the approach should be first considered from a wholistic perspective before looking at the individual component parts.	Yes, the future demands for risk management in project generally and the new ISO standards considerations will collectively place demands on change.	My understanding of these practices is very much as it is written here.	I look forward to seeing how these aspects are applied in cybersecurity management of BIM-FM	Not so much a change, but I do think the link to a physical building attack should be qualified – given that access to attack HVAC systems etc. is not an inherent characteristic of BIM – and these risks exist anyway in automated/networked BMS installations	It has highlighted a need for a deeper concern about cybersecurity risks for building owners/operators, which should be more deeply considered at the earlier stages of projects. The difficulty is that the people involved in FM are seldom concerned with issues that will	I have a pretty much similar understanding of these concepts. But as above, don't focus just on cyber. Contractors like to print off drawing and pin them up on walls; what does that mean to the security of the information?

								impact on operations. Their focus tends to be on getting the project delivered and move on to the next project. Even within client/employer organizations, the FM people don't think about operational issues.	
Strategy Layer	The determinants of integrating cybersecurity in BIM-FM at the strategy layer are	Q3. Are these two categories relevant and valid to	Yes, if BIM-FM determinants has a specific	Yes. The BIM-FM application and the oversight of the cybersecurity	If the groups contain determinants that	Yes	I think they are however, does this also cover strategic	Yes, they are valid. The challenge will be to get people with BIM	Yes totally. The use of BIM-FM should also be

	categorized in two groups: ➢ BIM-FM determinants ➢ Cybersecurity Management Determinants	cover the strategic integration determinants?	focus on FM specialties	should provide the checks and balances of reality and planned/assessed application.	reflect the extent of best practice and have the ability for determinants withing those groups to interact, then this grouping is fine.		business objectives of utilizing BIM? Another level of detail you may already have considered relates to the organization. If this is a FM company then they will also have to consider the Cybersecurity management determinants of their client organizations – if they happen to be data companies then	Management understanding, to speak to people with FM management understanding, to speak to people with IT & Cybersecurity understanding. You'll probably find these 3 groups of people operate in different departments, under different management and budgets. It will require thoughtful "leadership", to get these 3	captured in the strategy derived from ISO19650-5 as it should cover the lifecycle of the information in all formats.

							this will be significant.	groups of people to agree the BIM-FM-CS determinants.	
	To improve the cybersecurity status of a BIM-enabled FM, the framework suggests the following BIM-FM determinants at strategy level: • BIM Leadership • BIM Strategy Development • Regulations & Standardization	Q4. As per the determinant's description table, Is this a valid suggestion?	Yes, absolutely	Yes. BIM Leadership requires Strong support and recognition at Board/Exec level, focus must be deemed significant. Failure to apply the value of the decision makers to the overall strategy will diminish the potential security results.	On the assumption that both the leadership and strategy functions are sufficiently outward looking and not just focused on the organizational internal	Yes	Yes Potentially – they could also be rolled into more generic 'digital' roles and functions.	Yes, it is valid. It would be interesting to see what "authority" BIM Leadership has over FM and IT, to pull in inputs from those departments (which as noted above, are typically separate/autonomous functions in organizations).	Yes, it is valid. But note that include the work that should be carried out as part of ISO19650-5. An often-large gap is risk ownership and supply chain assurance pre and post

				Clear mandate must be made from regulatory bodies to ensure understanding of the Risks associated with non-compliance. Regulations and standardisation are implicit, although disjointed at this time.	structures and issues, then this should be fine. Most cyber-security threats are externally originated. Regulations and standards are usually reactive to situations, so this may be thought of as a minimum best practice.			The organisations legal obligation to maintain, and provide a "safety file" (building record, building logbook, etc.) under health and safety regulations, is also probably dealt with by a completely separate person/department, which may, or may not be engaged with BIM, FM, or IT. They may need to form part of	contract so these 3 areas should include these.

								the “strategy`\” group.	
	To improve the cybersecurity status of a BIM-enabled FM, the framework suggests the following cybersecurity determinants at strategy level: • Prioritization • CS Value Identification • Organizational Modelling of	Q5. As per the determinant’s description table, Is this a valid suggestion?	Yes. However, the “Organisational modelling of security requirements” terminology should be explained to FM	Yes. Overall Risk Assessment will be determined by the priority given to the facility, against a National measured result. Values of the inherent risks need a detailed connection, possibly the benefits of the	Yes, however the modelling determinant does not seem to involve any actual computational modelling activities.	Yes	Yes – with additional comments as per above – this may fall under existing ‘digital strategy’ determinants.	Yes, its valid but I would imagine this is where the primary “tension” will occur. BIM-enabled FM benefits from “MORE” access to more information, by more people, to help support daily operational task,	Totally agree Considering the information management, protective markings and the use of meta data to use the protective markings in model object data, often there is only one part of a

	information Security Requirements			Digital-Twin concept as per current discussion. Practicality of the application in re-structuring and operational changes will move a significant effort into the budgetary aspect. Current trends and market pressures will make this a difficult aspect of the change.				and reduce time/cost, and improve safety. The priority or concerns for IT, would be the opposite – "LESS" access, to fewer people, with more restrictions, which would limit the beneficial use of information in FM.	model (M&E for example) that is sensitive but that shouldn't make the entire federated model sensitive. Being able to accurately redact and understand aggregation is so important!
	BIMCS-FM suggests that the strategic	Q6. Do you agree with	Partially. My approach	Absolutely. Significant in all BIM integration	This statement is true, but it	Yes	Yes – but not in isolation – cannot lose	Yes, I agree "communication" is key. But	Yes. Again, this isn't necessarily an

	Cybersecurity and BIM determinants have an interchangeable effect on each other, and hence, they must be approached by effective communication and collaboration amongst the responsible teams (e.g.IT & FM teams).	this statement?	would be to have a separate security function to manage oversee both IT and FM teams. This would present a single function responsible for the holistic manageme nt of CS	is the aspect of Communication and transparency. The oversight capacity does require the two-way assessment and application to get optimal results. Methodologies of communication will be placed on more agile methods during strategy and operational periods.	should also include external parties who may be carrying out IT or FM activities. Without the external party being part of this, the cyber-security will be compromis ed.		sight of business aims & requirements. Plus, in my experience Cyber Security has sat above functional teams to ensure appropriate overarching standards, processes, architecture etc.	communication only occurs where there is common understanding, and where both parties can understand the point-of-view of the other. And, as noted above, the “tension” between wanting to allow “more access”, versus wanting to restrict or provide “less access”, will require some careful thinking. People, in	IT/cyber problem and IT departments can’t mitigate all risks.

								general, don't want to spend the time carefully working through issues – they want the "quick answer". For the BIM people, it will be "open it all up". For the IT people, it will be "lock it all down". For the FM people it will be "we're used to working with poor, or little information, so we'll just carry on as normal".	

								For the Safety people, it will be a box-ticking exercise “have we complied”. To get “communications” beyond these typical “quick answers”, will require strong and knowledgeable leadership. It must be acknowledged, that there is a “sweet spot”, somewhere between the “open it all up” people, and the “Lock it all	

								down" people. That requires judgment calls and compromise, and this is where "leadership" will play a role.	
Performance Layer	The BIMCS-FM framework suggests that a number of performance related determinants are required to support and enable the strategic determinants. These include:	Q7. Do you agree that the top-level performance determinants affect the fulfillment of strategic determinants?	Yes, very much. I have seen it far too often where board representative do not grasp even the basics of CS and are often	Yes. The think-tank of Senior Management will demand a considerable capacity to embrace a broad knowledge of practical experience and implications and permit the awareness of	I would agree that the performance determinants have an effect on the strategic determinants, but the majority of	Yes. However, if they are not competent enough, they need to acknowledge it and seek advice for project.	I agree. As much as its important for functional units to be competent and knowledgeable, it is even more important for those in higher positions to have oversight and competent	I agree that somebody at the top, who controls the budgets, and has authority to instruct people on what to do, must be knowledgeable in these topics, and understand the relationship	Yes, as long as they include risk ownership.

	➢ BIM Senior Management Team Competency ➢ Cybersecurity oversight at board level		the weakest link in the chain that could be exploited. Therefore Board members should have the appropriate knowledge, skills and training to be able to perform this role effectively.	results at board/exec level. The real-values are required to demonstrate the comprehensive approach required to planning and methods required for application.	the performance determinants will be driven by lower level functions, not senior managers and board member.		management skills in both BIM, FM and information security.	between BIM, FM, IT, Safety, Environmental/ CSR, and users/customer experience, and how that ultimately impacts performance/outcomes for built assets. I'm not sure that directly means all these people have to be "board level". But certainly, part of the management team. It will depend on the organization	

								size and structure, I suppose.	
	The BIM-CS framework suggests that for a successful integration of cybersecurity in BIM-FM at a strategic level, two performance related determinants must be taken into consideration: ➢ BIM Senior Management Team Competency	Q8. As per the determinant's description table, Is this a valid suggestion?	Yes, please see my comments above.	Yes. The dual interaction is important to retain impartial oversight within the two entities, both have capacity to influence the other. The current capability of Senior BIM management will be challenged with the initial implementation of CS.	The high-level teams (board and managers) will only enable better performance. Successful integration is achieved by those actively involved in the activities, who are generally at	Does the BM senior team need to be competent in CS if they ensure that they collaborate with cyber security? Agreed you want full support from the board	Yes – again we are focusing on BIM, but I would expect this to sit within framework of wider digital focused determinants.	See answer above.	Surely. BIM is as much as a business change process as it is about cyber security; so that needs to be understood at board level and controlled/managed throughout the organization and relevant stakeholders.

	➢ Cybersecurity oversight at board level				a lower pay grade.				
	BIMCS-FM suggests that the development of a cybersecurity minded organizational BIM strategy leads to the employment of cybersecurity embedded trainings and	Q9. Is this statement valid?	Yes, agree	Indeed.Training is required in all processes in BIM applications. The need for this is enhanced by the technologies employed and the considerably different environment in design and	Yes, training and education are critical and should be applied in a rolling manner to keep skills updated as threats	Yes	Yes – but organisations that operate digital business platforms should have this in place anyway	Yes. Upskilling of people at all levels will be required. Personally, I think the "technology" should do as much of the management as possible, because people are lazy, and	Yes, again don't focus on cyber. BIM is a way of working and needs a more holistic approach. Cyber is 'one layer'.

	educational programs.			documentation projects.	metamorph ose.			prone to mistakes/errors. Many cyber security breaches originate through the stupidity of people.	
	BIMCS-FM suggests that the implementation of cybersecurity minded BIM strategies depend on three performance centric determinants: ➢ BIM knowled ge & skills	Q10. As per the determinant' s description table, Is this a valid suggestion?	Yes, with oversight from the board.	Yes.Current trends and practice, do not consider the impact of the CS requirements. Raising awareness of the risks and developing that awareness will be a major effort, across all	Yes. Knowledge , skills and culture are enablers of performanc e. I could know and want to achieve all sorts of things, but if I don't	Yes, with the condition that at the beginning of the implementa tion there may be little or no knowledge of this – a capability	Yes	I agree but I think "Risk Aware" culture, also has to be balanced with "Reward Aware" culture – an understanding of the benefits of BIM to the organization, in terms of Cost,	Yes, in a way to prepare the organisation for dealing with business change

	➢ Cybersecurity knowledge & skills ➢ Risk aware culture			projects, and even early application on significant projects. The operational requirements of the environment, is significantly different from current practice. Implementation will require a detailed appreciation of the impact on production/productivity. BIM knowledge and operation is one level where	do those things, my performance will be zero.	maturity model might have a score of 0.		Time, Safety, Performance, Outcomes, user/customer experience etc. Without considering the "rewards", the risk adverse people will "lock it down" and make the use of BIM difficult.	

				the current trends are for easier and less rigorous checks and balances, and managed by the "system", so a greater focus will need to be placed on people.					
Implementation Layer	BIMCS-FM suggests that for improving cybersecurity of BIM implementation in FM, two groups of determinants should be considered: BIM FM determinants	Q11. Are these two categories relevant and adequate to cover the implementational integration determinants?	Partially. Assessment of Risk is also required	Yes. Specific consideration should be made for the needs of the operation and require an open approach to methods.	Generally, yes, but as with everything in life, there will be externalities that will also have an effect on this area.	Yes	Yes however I don't think FM and CS can do this in isolation from the business. The FM function and BIM specific tech should be engaged through the wider digital	Agreed but I see a few different groups under BIM-FM and CS who are involved in activities related to FM, BIM, Health and Safety, Customer relations, etc. and it differs	yes

	Cybersecurity determinants						business strategy.	from one organization to another.	
	To improve the cybersecurity of BIM implementation in FM, the framework suggests the following BIM-FM determinants at implementation layer: • Defined BIM-FM processes	Q12. As per the determinant's description table, Is this a valid suggestion?	Yes, the pre-tender competency evaluation should be done from a cyber security point and information management	Yes The ISO 19650 strong standard is a good foundation to ensure better process. Currently larger projects, and Professional project teams have better capacity, but only in significant projects; based	I read the determinants as saying "if we know what we are doing, how we are doing it and those we are doing it with are capable, then we are fine", then	Yes it is valid. FM needs to explore on what basis are the processes audited and how are the suppliers assessed for their competency.	Agreed – and not just competency assessed pre-tender but also testing of product and management security standards	Yes. Valid suggestions. I think "technical solutions" should also be specified. They may form part of defined processes, but should be defined. Technical solutions, that help people to fulfill their	Very much so – but link it to the ISO19650-5 work that *should* have been done.

	• BIM Infrastructure maturity • Defined Information Requirements • Monitor & Audit Processes • Pre-tender BIM competency evaluation		competency	on cost and scale. The larger cross-section of projects managed by smaller, less sophisticated users have a large potential impact on a wide-based coverage. Audit processes are very important and will demand additional skills and awareness for the operational aspects. The consideration of strategy is to	this is a valid suggestion.			obligations defined by the processes. People are lazy by nature, and forgetful, and the technology should be there to make "compliance" as easy as possible. "user-focused" technical solutions, where all the "complexity" is built into the back-end of the system.	

				have understanding of the impacts. Measures need to be made open to the market to raise general awareness and corrective action. Measures for competency are already difficult in the BIM environment, the FM additional requirements are an extra load with impact on evaluation procedures. The evaluations need to be					

				implemented at the earliest opportunity to ensure even compliance and not overloaded events in the timeline.					
	To improve the cybersecurity status of a BIM-enabled FM, the framework suggests the following cybersecurity determinants at strategy level: • Cybersecurity design • Risk management plans	Q13. As per the determinant's description table, Is this a valid suggestion?	Yes, if the risk management plans and defined processes are well communicated with everyone in the organisation	Yes. The systems development needs to provide a framework to manage the extents of the planned security. The balance of the design and the implementation in strategy is to determine the real capability	Assuming implementation; plans and processes are fine but checking that these plans are being carried out in an appropriate way will	Yes but more detail is needed as to what these are to ensure consistency. Risk management plans are different within every organizatio	Agreed – and all must be reviewed constantly against wider industry development. For example hardware may have been built using chipsets that have since been compromised,	Yes. Valid Suggestions. Again, I think "technical solutions" must be considered, to find the right balance between giving the right people, the right access to information, at the right time, in an easy way,	Yes, the only suggestion is that there is a bit of over-use of the term cyber security.

	• Defined security processes			balanced between reality and anticipated/planned. The over/under capacity, will have large impact on the practical nature of the security. Applicable actions and real results will influence the overall performance more than anything.	also be important to close the information loop.	n and it needs to have some sort of consistency.	similarly for code in software – hence periodic vulnerability testing.	without compromising the cyber security. Don't leave the "design" to the IT people alone, as they will "lock it all down", and make things difficult for people.	
	BIMCS-FM suggests that the	Q14. Do you agree	Yes, but managed	The inter-relationship of	Absolutely, communica	Yes the collaboratio	Yes –I would expect this	Yes. This should be	Yes

	Implementational Cybersecurity and BIM determinants have an interchangeable effect on other and hence, they must be approached by effective communication and collaboration amongst the responsible teams (e.g.IT & FM teams).	with this statement?	by security team	the two aspects in clear.The strategy needs to consider the practical issues that exceed the IT and FM teams. Including the management of physical documents and access/security of the working environments, especially in the light og BYOD and remote working trends, which are due to increase.	tion between teams will always be critical to implementation.	n and effective communication is whats missing from the organisations who are dealing with digitization	collaboration to be wider than just BIM. In some organisations this might be IT to FM directly, in others IT and FM might be 2 of several representatives under an overarching CS oversight.	considered carefully, especially where there are strong competing perspectives, where a level of compromise has to be reached. Any “dominant” party (either in authority, or personality) in the negotiation, could skew the outcome/results to be less optimal. The “implementation” should be seen as an “agreement” or contract,	

								between the departments/players, ultimately signed off by the leadership of the company (who are the ones that are going to be sued/penalized, when a breach occurs).	
	BIMCS-FM suggests that the results of the monitoring & auditing should be communicated at every level, to enable improved decision making	Q15. Do you agree with this statement?	Yes agreed.	Yes.A wholistic review process need integration from the strategic level to the group operational level with real reporting and transparency to all users. The	Yes.Auditing can be a blunt tool; those being audited will cast the best light possible on whatever activities	Monitoring and auditing should be done using technology(real-time). Otherwise it will not	Yes – the specific message / information may well be different depending on audience, but all levels	Monitoring and auditing should as far as possible be provide through "technical solutions", that leverage technologies like AI,	Yes. Understanding the security maturity landscape across the supply chain is essential

	at the top that ultimately feeds improvement into all processes and procedures.			relevance is then tangible and direct resulting in improved levels of awareness.	are being scrutinized. On-going monitoring is usually the better option, but does not usually generate the granular feedback that higher manageme nt functions are looking for, hence we have audting…	have the results which is required to control and manage the cybersecuri ty	should be included.	Machine learning, blockchain (ledger) etc. so it is “real-time”, and issues are flagged often etc, and management “dashboards” are available. Manual auditing and reporting tends to be less effective, and only surfaces high-level issues. A cyber security breach needs to be known straight away, not at the end of the	

								month, or end of the year. Continuous improvement will be assisted, where smaller, daily tasks are given to people, rather than large, daunting tasks. And if completion, and sign-off of these are assisted by “machines”, and even linked to payment incentives in contracts, there is a better chance of achieving results.	

	BIMCS-FM framework aims to assist the facilities management organisations to implement a cybersecurity minded approach to the adoption of BIM.	Q16. Do you believe the BIMCS-FM brings value to the cybersecurity minded adoption of BIM in FM?	Absolutely. The FM and construction is usually all about optimizing operations and functionality and forget about the more important aspects brought by the deployment of tech and	FM lacks awareness, skills and understanding of the way it can contribute to the security of information. The general understanding of cyber is that its not something they need to take care of. The IT and security commonly manage this aspect, despite the fact that those departments will not have	I have been actively engaged with standardisation and what I have observed over the years is that security is and has always been an adhoc. It has never been treated as part of the job and the way this	My experience with leading FM organisations was that they struggle to find where to start with their security journey. The structure and layers proposed would simplify the process of creating a	Yes. The value of the suggested framework for the FM goes beyond cybersecurity in BIM and would assist with a better management of processes and procedures within a digitally enabled organisation.	The application of the framework in organisations (and particularly small and medium) would require time and effort to build the foundational knowledge, skills and structural divisions. However, it holds great potential to improve on the security mindedness of BIM projects in	Yes. Surely This work presents a wholistic view on the issue of cybersecurity management, while paying attention to the individual elements that contribute to a better management of this issue.

			digitalizati on.	sufficient knowledge of the operational needs. What this framework suggests in terms of the integration of security in operations sets a road map for FM to follow.	framework has pictured the elements and how they connect would make a difference in perspective and how info security is viewed within FM and BIM projects.	more secure FM through implanting and mastering the proposed factors.		operations and maintenance phase.	