BIM Enabled Facilities Management (FM): A Scrutiny of Risks Resulting from Cyber Attacks

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

Paper type- General review

1. Introduction

In recent years, the digitalisation of the architecture, engineering, construction and operations (AECO) industries, has led to drastic transformations in the way information is generated, communicated, stored and used (Chen *et al.*, 2020; Davtalab, 2017). The development of digital platforms that facilitate stakeholders' collaboration, paired with digital tools such as building information modelling (BIM) has brought an extensive range of benefits to those involved with the planning, design, construction, operations and maintenance phases of a project (Davtalab, 2017). As per Pishdad-Bozorgi *et al.* (2018), BIM particularly benefits facilities management organisations, by providing as-built information of the facility, and enabling digital handling, exchange and storage of data for operations and maintenance of the facility. As stated by Chen *et al.* (2020), the full adoption of BIM within a facilities management organisation will enhance collaboration between various stakeholders of a project, through presenting an up-to-date model of the facility with all the required information. In light of this, Naghshbandi (2016) states that BIM will optimise the processes by reducing the time and human resources required for undertaking tasks within a facilities management organisation.

The benefits of adopting BIM are greatly acknowledged within the industry and academia; however, there are also discussions around the challenges associated with such technologies. As per Boyes, (2014a), one of the key challenges associated with the use of BIM is the issue of cybersecurity. With the implementation of BIM within the facilities management organisations, and the increased use of smart devices within facilities, buildings are now susceptible to a range of cyberattacks (Boyes, 2015a). In light of this, Mayo and Snider (2016), articulate the heightened risks of security compromise that threatens BIM enabled facilities and their managing organisations. Therefore, it is important to protect the built environment from cyber intruders who wish to compromise the integrity, confidentiality and availability of digital information (Kelly *et al.*, 2013). Any compromise of information security would inherently lead to the compromise of the potential benefits of BIM that the organisation were seeking. Therefore, this paper investigates the BIM benefits in facilities management organisations and the potential implications of a cybersecurity breach in the accomplishment of such benefits.

2. BIM for FM: realities and shortfalls

As per Then's, (1999) description of facilities management, it is a practice that seeks to provide a functional environment for the support of businesses and their resources. ShiemShin Then (1999)elaborates about the role of facilities managers, balancing all assets inside a facility by delivering the needs and overcoming the challenges. 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). Many resources such as the OmniClass Construction Classification System (OCCS) distinguish between the management of facilities and their operations and maintenance tasks (Services, 2018). In fact, early research (e.g. Barrett and Baldry, 2003; Becker and Steele, 1990) on FM have focused on safety, functionality and usability of facilities, as part of the operations and maintenance, which supported acknowledging part of the complex nature of FM. From another perspective, other authors have even proposed that facilities management can also include all the stages of a construction project (Ebinger and Madritsch, 2012). Volk *et al.* (2014) and Patacas *et al.* (2015) point out that with the implementation of BIM in facilities management organisations, the coordination of all phases of the construction project will be possible through early engagement of the facilities management with the project. This engagement would assist with better implementation of workflows, tools and regulations to define the information requirements of facilities management tasks (Abdelmohsen *et al.*, 2011). The use of BIM in FM was based on the Industry Foundation Classes' (IFC) standards, which was later modelled by Yu *et al.* (2000), who mapped the IFC and FM requirements through data modelling. The coordination of all phases of a construction project with the operations and maintenance requires flexibility that enables optimum change management. Kang and Choi, (2015) assert that BIM facilitates this flexibility by accommodating various scenarios and project requirements. Having large volumes of data generated and exchanged between different stakeholders, Becerik-Gerber *et al.* (2012) point out the cybersecurity vulnerabilities of information due to a lack of synchronisation amongst the information sources. Affirming the above, Korpela *et al.* (2015) highlight the capability of BIM to overcome such issues. In doing so, BIM information requirements are fully defined to accommodate FM coordination with other phases of the project. As per Carbonari *et al.* (2018) using BIM inherently improves on the operations and maintenance procedures, by providing access to all the required information through a digital platform.Henceforth, understanding the information requirements of each task enables improved access management, limiting the access of users to only the data they require to undertake that specific task. This would inherently reduce the risk of unauthorised access to sensitive information, as well as saving the time it takes to find task-specific information. In a study by Gao and Pishdad-Bozorgi, (2019) ,the purpose of BIM implementation in FM was to enhance communication and collaboration amongst all stakeholders. Similarly, the work of El Ammari and Hammad, (2019) proposed a model in which data was captured from various sources to assist with the operations and maintenance tasks on site, by enabling remote access to information for the FM teams. In this regards, Hu *et al.* (2018) point out the importance of having access to the mechanical, electrical and plumbing (MEP) updated as-built information, to perform operations and maintenance tasks and assert the role of BIM in simplifying access to the required information. Another study by Chen *et al.* (2018) proposed automatic scheduling using BIM in FM, with the aim of optimising resources required for every task. In light of the optimisation that can be facilitated by BIM, Chen *et al.* (2020) also developed an alternative model in which the challenges of integrating BIM in FM were investigated, and a model was proposed to assist with enhancing productivity using BIM in FM. Facilities management organisations are involved with the management and maintenance of assets, both tangible and intangible (Atkin and Brooks, 2015). 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), sustainability projects in the built facilities and those projects involving refurbishment and renovation can neither be fitted in operations nor management. Hence, space management is considered as an individual category which includes management of space and optimising the utilisation of facilities' environments. Hence, FM task areas are categorised into three: asset management, space management and operational management. Each task area is involved with the management of certain aspects of a facility.

2.1 Financial Asset Management

Facilities management is not only limited to managing and maintaining the physical assets of a built environment, it covers the management of all assets related to a built facility (Guillen *et al.*, 2016). The asset management task area is involved with managing the finances as well as the facilities' contractual documentation and legal matters. 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, 2016). For an optimum management of assets, data should be collected and maintained for all systems and services that are continuously running to keep the building functional. Asset management is responsible for 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 more asset specific information that assists with effective management of the physical (tangible) and digital (intangible) assets related to a facility (Becerik-Gerber *et al.*, 2012). Managing finances and budgetary controls carried out as part of asset management work requires concise information about material quantities, and the labour costs required for undertaking a specific task. BIM has the potential to provide accurate information that can be used for making informed decisions on the budgetary plans (Tang *et al.*, 2020). This is sometimes accompanied by challenges regarding the interoperability of information models with all the other organisational asset information system(s). Therefore, information requirements should be set out by the facilities management early in the projects, to ensure the delivered information models are compatible (Pocock *et al.*, 2014). Consequently, the availability of accurate information in BIM enabled facilities management would inherently enhance the assets' value by enabling effective facility management (Guillen *et al.*, 2020). This is achieved through effective management of budget and human resources and timely maintenance of the facility, which improves the life-span of the built asset (Alkasisbeh and Abudayyeh, 2018). However, it can be stated that majority of research on BIM for FM, with those that particularly looked into asset information (e.g. (Guillen *et al.*, 2016; Patacas et al., 2020), have limited focus on what data / information are critical / sensitive, hence lack of understanding security-related concerns to many of the assets in an organisation.

2.2 Space management

Space management involves the optimisation of the way space is used. In light of this, Steiner, (2006) adds 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. 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 assets' description along with the status of the space being used or left un-used. 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, sections' modelling, layout views and visual rendering of the proposed changes; and hence, results in time and cost-efficient decision making (Love *et al.*, 2014). Another desirable features of BIM is its capability in visualising space and its components, enabling optimised planning of the requirements of space utilisation (Becerik-Gerber *et al.*, 2012). An additional benefit of BIM in FM is the potential to monitor assets' utilisation during their use period. This would assist with understanding if the space sufficiently and efficiently meets the users' requirements (Ashworth *et al.*, 2016). Although many efforts have attempted to illustrate the application and value of BIM for FM, with many researchers and practitioners continuing to seek an improved understanding of space-related consideration within FM, there exist a number of challenges. One of the identified challenges in this regard is inconsistent labelling and updating of information, which can be resolved by standardisation and effective application of BIM in FM (Becerik-Gerber *et al.*, 2012). Although such issue was picked up in recent research work by Patacas et al. (2020) where a framework was proposed to encompass holistic consideration of Asset Information, the focus on how this can impact space management with indicating what data / information require careful handling were not explored. For the existing buildings where the BIM model lacks a structured set of data integrated within, lack of geometric information and 3D models that suit space planning and reporting might cause complexities for the FM organisations (Hoang *et al.*, 2020; Naghshbandi, 2016).

2.3 Operations and maintenance

According to Barbarosoglu and Arditi, (2019), operations and maintenance take two forms: corrective and 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.*, 2015; Sullivan *et al.*, 2010; Yam *et al.*, 2001). The use of digital technologies within the FM task areas has many advantages (Pishdad-Bozorgi *et al.*, 2018). A number of digital tools are currently used to optimise FM working processes, examples of which include: Computer Aided Facilities Management (CAFM); Computerized Maintenance Management Systems (CMMS); Electronic Document Management System (EDMS); Enterprise Asset Management (EAM); Building Automation System (BAS); Integrated workplace management system (IEMS); ECodomus (Cloud based software for Visual Facility Management); and FAMIS (Facility Administration and Maintenance Information System) (Davtalab, 2017; Kelly *et al.*, 2013). The implementation of BIM within facilities management organisations is still at its infancy; however, it has the potential to link and bridge with the abovementioned digital solutions that are already operating within various facilities management organisations. 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, leading to an optimisation of processes and work plans. When coupled with BIM, they allow a real-time exchange of facilities' information with all stakeholders involved. Furthermore, BIM provides access to information about the buildings' structure and shell, entailing the load calculation for structural elements (column, beam, slabs, core wall and shear wall) and assisting facility managers in decision making about 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). In maintenance management, BIM assists the facility management 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 the facility management to undertake a risk assessment for operation and maintenance processes, leading to improved coordination amongst the contractors, suppliers and interorganisational teams (Becerik-Gerber *et al.*, 2012). Furthermore, operational management requires continuous and real time monitoring of the facilities, which is where BIM plays a critical role. The real-time sensing of the equipment integrated with BIM 6D-models can save time by up to 80% (Davtalab, 2017), enabling optimisation of processes and procedures. In addition, the building performance data collected through BIM ensures that the building is operating as per a specific standard. The areas in need of modification and upgradation can be identified by the facility management team to improve the overall building's performance (Carnero and Gómez, 2017). The accurate assessment of the asset including the resources' limitations and the conditions of the asset assists the facility management team to model and predict the deterioration and depreciation of the assets. Further, the repair and maintenance strategies can be selected by also taking into account the requirements and risks involved in the processes (Naghshbandi, 2016). 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 buildings' behaviour and facilities' deterioration more accurately. However, Koch *et al.* (2014) believe that there is an issue with the availability of information in standard digital format that can be integrated into BIM databases. In traditional facilities management, equipment details, data sheets, spare parts, maintenance schedules and all the information required for undertaking FM tasks were generated and updated manually. Manual entry or upgrading of information is prone to human error resulting in the compromise of accuracy, real-time availability of information and their integrity (Keady, 2013). With the use of BIM in FM, these tasks will be digitalised to improve on the data accuracy and availability, as well as optimising the work processes by reducing labour and time (Gu *et al.*, 2008). However, having all the data on a shared digital platform is associated with increased vulnerability towards cyber-attacks, which would impede the benefits associated with the use of BIM.

In light of the discussions above, table 1 below showcases the benefits associated with using BIM in various task areas of FM, which include but are not limited to what is presented below:

[Table 1 here]

3. Cybersecurity of digital data

Cyber-attacks are commonly known to adversely affect the functionality of computer systems (Nye, 2018). Sharma *et al.* (2010) also provided a similar definition in which he defined a cyber-attack as any outside attack that could compromise the security of an organisation or a system inside the organization. Cybersecurity threats can hugely impact organisations, assets and people involved (Von Solms and Van Niekerk, 2013). Malicious cyber-attacks are acts carried out with the intent of destroying data or documentation for the users (Mayo and Snider, 2016; Wood, 2000). A malicious cyber-attack, if successful, allows unwanted access to unauthorised actors, resulting in potential loss of information integrity (Boyes, 2015a; Mantha *et al.*, 2020). There are also non malicious acts that threaten the confidentiality, integrity and availability of information within a system. For instance, if access is mistakenly granted to an unauthorised employee outside a project team, any intentional or unintentional change in the data leading to serious implications is counted as a cyber-breach (Mayo and Snider, 2016; Sommer and Brown, 2011). There are different forms of cyber-attacks which might cause damage or disrupt the assets (Peng *et al.*, 2013). The different threats include intellectual property theft, degradation of assets, malware, viruses, worms, and spyware (Marinos, 2013; Szyliowicz and Zamparini, 2014). Similar to physical assets in which they can provide protection to occupants against threats (Alguliyev *et al.*, 2018),IT infrastructure assets should also provide security to users against potential threats and attacks. It is difficult to keep track of cybersecurity risks that could affect digital collaborative solutions, especially with all the daily increasing threats. Risks related to security depend on the system’s structure and how it is used.

There are advanced technologies that would help in monitoring and operating assets such as smart networks that are equipped with sensors (Lin *et al.*, 2007) and intelligent computers with advanced computational powers (Pärn *et al.*, 2017; Pop *et al.*, 2015).These technologies could help in providing insights and propagating knowledge (Pärn *et al.*, 2017). The use of digital collaborative solutions could also help via economic benefits in the form of increased profitability for organisations (Lin *et al.*, 2007; Ryan, 2017). This has driven governments to encourage organisations in the AECO sector to embed digital solutions, such as digital collaboration environments while working on projects. Although digital collaboration environments help in better collaboration and communication in addition to cost savings (Bradley *et al.*, 2016), they create a window for cyber-attacks and threats to systems as a result of their centralised and highly connective nature (Boyes, 2014a). Cyber-attacks could have adverse impacts on the data processed in the virtual environment and might have disastrous effects on the infrastructure asset (Parn and Edwards, 2019). Unauthorized access to sensitive materials can jeopardise security of systems which could have an amplified effect when they happen in the cases of critical infrastructures (Liu *et al.*, 2012). As such, organisations and governments have established methods of defence such as firewalls (Mayo and Snider, 2016), and protection gateways (ANSI, 2007). However, all these efforts cannot guarantee that cybersecurity is intact. All the previously discussed technological solutions have several advantages but they are subject to cyber-attacks and risks which make them vulnerable. This could be attributed to their heterogeneity and due to the fact that there might be private sensitive material which is handled through these technologies. Hence, cybersecurity risks should be identified and treated through a strategic approach.

4. Cyber security in the built environment

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 the facilities management entails a bridge between the physical building and its intangible assets. Traditional facilities management targets managing the physical aspects of buildings such as fire safety, equipment safety, physical security, and much more (Enoma *et al.*, 2009; Leung *et al.*, 2005). However, security of cyber spaces and digital networking systems and platforms is commonly disregarded and overlooked within the AECO industry (Parn and Edwards, 2019). An in-depth consideration of cybersecurity attacks has shed light on the fact that a malicious intrusion into a cyberspace is often associated with a physical target and leads to physical harm. The combined physical and cyber impact of such attacks has caused uncertainties in cybersecurity risk ownership amongst the facilities management organisations (Ghosh *et al.*, 2019). The lack of cybersecurity expertise amongst the FM professionals further exacerbates the vulnerability of their systems to such attacks. This is mainly due to the lack of a cybersecurity minded interaction with systems and tools (Boyes, 2015a).

The built environment is not exempt from the eminent threat of cyber actors and hence, the facilities management organisations, in particular, the BIM enabled FM organisations capable of real time managing of buildings and facilities must incorporate cybersecurity considerations in their work plans (IET, 2013). A cybersecurity threat to BIM enabled facilities management is heightened by the digital collaborations brought by BIM. However, the cyber risk impact is exacerbated due to the existing connection with building building management systems (BMS) (Mayo and Snider, 2016; Minoli *et al.*, 2017). An unauthorised access to systems as such can lead to disastrous outcomes for the facility and occupants by causing disruption to services, or resulting in a loss of control, leading to serious health and safety harm to the occupants (e.g. disabling fire alarms can have life threatening implications in a fire incident) (Boyes, 2015a; Parn and Edwards, 2019; Purpura, 2019). This illustrates that the impact of a cyber-attack in BIM enabled facilities management results in complications beyond the cyber world. The facilities management systems encompass information about the physical attributes of a building. BIM facilitates a holistic view into the details of a building, a golden thread of information that attracts malicious cyber actors. BIM enabled facilities management further requires a common data environment for stakeholders' communications. An attack to the common data environment can act as a vector of attack to the FM control systems. 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); to exemplify, access to BIM data can expose details of CCTV specifications and locations, easing the way for the 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 unauthorised viewing of images, or tampering and altering images to compromise the information's integrity (Abie, 2019; Boyes, 2015b).

Therefore, the implications of cyber-attacks and their impact on the tangible and intangible assets related to a facility need to be understood by the facilities management team. However, the multi-faceted nature of the problem does not match the existing competencies of the facilities management organisations. Hence, it is important to investigate the impact of cyber threats on buildings to provide an insight into "what can go wrong", in order to establish the importance of understanding, managing and preventing cybersecurity risks in BIM enabled facilities management.

5. Methodology

The construction of this paper is based upon a thematic review of the existing literature in the domains of cybersecurity and BIM enabled facilities management. As per Braun and Clarke, (2012) and King *et al.*, (2004), a thematic exploration of the phenomenon enables focused research of multi-disciplinary concepts, without the complexities of a systemic exploration. This research was hence approached by the review of peer reviewed published resources and the analysis of the knowledge extracted from the literature. A total of 233 peer reviewed publications were found using electronic database search engines, including Google Scholar and Science Direct, within the two domains. From all the resources identified, 90 were selected based on the research criterion. The criterion entailed the selection of cybersecurity resources discussing cybersecurity from a non-technical viewpoint, in the domain of the built environment. The key phrases used for this search include "cybersecurity", "cybersecurity in buildings", and "cybersecurity in BIM", where the latter had very little turnaround. Furthermore, the selection of BIM resources was based on their focus on the post-occupancy phase, and in particular, facilities management organisations. Key phrases for this search include "BIM in FM", "BIM benefits in FM" and "advantages of BIM". This resulted in 65 resources in the cybersecurity domain and 25 in BIM being selected for review.

The review of the literature was first conducted to achieve an overview of the underpinning reasons for implementing BIM in FM. For this, the potential benefits of BIM in FM were reviewed and categorised in their associated FM task areas, including asset management, space management and operations and maintenance management (Figure 1).

[Figure 1 here]

The availability of literature on the issue of cybersecurity in BIM and in particular, BIM enabled facilities management was found to be very limited. Cybersecurity in the context of the built environment is commonly focused on the cyber-physical systems in the buildings, and their connections with the facilities management systems, such as BMS and CAFM. Hence, the issue of cybersecurity within BIM enabled facilities management is addressed by first looking at the implications of a cyber breach on buildings, taking into consideration the existence of IoT devices within most buildings and facilities that are connected to a building/facility management system. The application of BIM in FM and its connection with facilities management systems were then discussed by listing the benefits associated with the use of BIM. The list includes benefits to the facilities management organisation as well as for the facility itself.

Hence, a multi-disciplinary analysis of the literature resulted in gaining an in-depth insight into the impacts of a cybersecurity breach in BIM enabled facilities management, on the buildings and their managing organisation. Based on the cybersecurity triad, namely the confidentiality, integrity and availability (CIA) of information, the findings of the literature were structured to showcase the cyber risk impacts in BIM enabled FM. The cyber risk impact matrix in BIM enabled FM indicates the criticality of the issue, using the BIM benefits that will be compromised as a result of a cyber breach. The outcome of this study highlights the importance of investing in improving the cybersecurity management capabilities of BIM enabled facilities management organisations. It also provides a base for future research into the measures of cybersecurity risks with respect to various characteristics of BIM enabled facilities management organisations.

6. Results and findings

Findings from the comprehensive review of the literature in the domains of BIM and cybersecurity in the built environment revealed that within the lifecycle of a BIM project, with the progression of the project to higher levels, the level of details (LoD) of content and the volume of information that is generated and stored increases (Hooper, 2015; Ikerd *et al.*, 2013; Leite *et al.*, 2011). Hence, in the build and post-occupancy phases, the LoD is significantly higher than the concept planning and design phases. Also, the literature review suggests that the post-occupancy phase has the highest percentage of as-built information stored and exchanged for day to day management and maintenance of the facilities (Mandhar and Mandhar, 2013; Matarneh *et al.*, 2019; Patacas *et al.*, 2016). Although this phase is only one of the four main phases of the project, it goes on for the longest duration of time in comparison to the other phases of planning, design and build, which would only take a small portion of the whole life span of a project (Kensek, 2015; Terreno *et al.*, 2016). The literature has suggested that information that is archived and exchanged at the post-occupancy phase within the facilities management managing the facility, would last for an average of ten years, and would be exchanged amongst a large number of stakeholders (Ebinger and Madritsch, 2012; Kim *et al.*, 2018; Matarneh *et al.*, 2019). In many cases, the literature has also shed light on the change of the facility manager organisations, at multiple points within the life of a facility. Hence, this suggests a complete transfer of all data and information to the new facilities management organisation in charge (Codinhoto *et al.*, 2013; Edirisinghe *et al.*, 2017; Kadefors, 2008; Sridarran and Fernando, 2016). Therefore, having a large volume of data, archived and exchanged between numerous stakeholders for a long duration of time, creates maximum vulnerability to an information security breach. Hence, it can be concluded that the cybersecurity vulnerability is at its maximum in comparison to other phases of a BIM project's life cycle.

Considering the naïve approach of the AECO industry and specifically the facilities management in managing the cybersecurity risk, the literature indicates that most organisations tend to have a technology focused view of cybersecurity and over-rely on technological solutions and technology providers. The lack of knowledge and awareness of secure handling of BIM data was also identified within the literature. A lack of coordination across all stakeholders involved in various stages of a BIM enabled project, inconsistency of processes, lack of compliance and interoperability weaken the security of information that is exchanged across all organisations. The literature also accentuates the importance of the competent management of cybersecurity and criticises the silo IT focused approach to overcoming this issue. Many researchers have emphasised the importance of a risk aware culture, which is currently lacking amongst many AECO organisations.

The review of the literature in the domain of cybersecurity in the built environment, has shed light on the various cyber breaches to the digital environments and platforms that facilitate the exchange and storage of information. The integration of advanced IoT devices and their connections to various networks and building management systems linked to BIM platforms, suggest an increased vulnerability of the built environment to cyber-attacks that target the safety, security and integrity of the buildings and facilities. At the post-occupancy phase of a BIM project, the information that is exchanged and stored is of a high level of detail which entails the as-built data of components and structures of the facility. The inclusion of IoT devices within the built environment enables malicious cyber actors to perform cyber-attacks, with the aim of incurring physical damage to the facility and/or its occupants' health and safety. Such malicious acts can compromise the confidentiality, integrity and availability of information, which would inherently cause damage to the facility and the facility management organisation. The damage can take the form of financial loss, reputational loss, operational disruption, security breach, injury or loss of life of the occupants. Hence, the impact of a cyber-attack at the post-occupancy phase of a BIM project is deemed as critical. The development of the BIM life-cycle cyber risk model (Figure 2) portrays various phases of a BIM lifecycle and their attributed LoD (Alavi and Forcada, 2019; Cassano and Trani, 2017; Hong *et al.*, 2019; Hooper, 2015; Ikerd *et al.*, 2013; Nilsen and Bohne, 2019), information content (Akcamete *et al.*, 2011; Bryde *et al.*, 2013; Hjelseth, 2010; Ikerd *et al.*, 2013; Lea *et al.*, 2015; Patacas *et al.*, 2016) and potential cyber risk impacts at each phase (Abie, 2019; Dunn Cavelty, 2005; Griffin, 2019; Kabanda, 2018; Khajuria *et al.*, 2017; Wamala, 2011; Wood *et al.*, 2019). It also demonstrates a holistic view on the issue of cybersecurity, by presenting the risk impacts at each stage and clarifies the life span of each phase to enable comparison.

[Figure 2 here]

The model illustrates that although the cyber risk impact criticality is not as severe as other phases of planning, design and build, the risks of a cyber-attack at each phase can still have disastrous effects on the facility and those involved in the project. However, the post-occupancy phase is found to be the most critical in terms of the impact of cyber-attacks. A summary of the factors that support this finding are as follow (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) :

i. Very high volume of data is exchanged and stored in the facilities management organisations

ii. A long-term (more than 10 years) of data life cycle is estimated for the operations and maintenance phase.

iii. 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.

iv. Increase of physical Security risk as a result of smart devices and sensors installed in the buildings, which can inherently cause danger to the health and safety of personnel and residents of the facility.

7. Discussion

7.1 Cybersecurity for the built environment: the ambiguity of people and process

BIM facilitates a collaborative approach towards the generation, utilisation and management of digital information models of a physical asset and its attributed operational characteristics. When effectively coordinated to its optimum capacity, BIM can support real-time decision-making using object-based modelling technologies (Ghaffarianhoseini *et al.*, 2017). However, for achieving the full potential of BIM, radical changes are required amongst the procurement methods and contractual frameworks, as well as a culture shift towards a digital data driven approach to construction projects (Zhang *et al.*, 2015). The hinderance of the role of people and process in favour of technological excellence has resulted in an immature approach towards the adoption of BIM (Hetemi *et al.*, 2020). Most organisations within the AECO industry are overly focused on the technological advancements brought about by the notion of BIM, without realising the vitality of fundamental strategic plans and standardised processes (Lea *et al.*, 2015; Mom and Hsieh, 2012; Sackey *et al.*, 2013). Lack of a strategic approach to the adoption of BIM leads to inconsistency in working processes; poorly maintained technologies and devices; ambiguity over roles and responsibilities; lack of defined information requirements; poor employee performance; and a silo approach towards the management of technological aspects of the business (Ashworth *et al.*, 2016; Boyes, 2014b; Gu and London, 2010; Sommer and Brown, 2011).

Findings of this research showed the need to provide more focus on people and process sides with relation to cybersecurity. For instance, from a process perspective, lack of defined information requirements for FM would lead to the exchange of a large volume of facility related data amongst the stakeholders, without considering the relevance of those information to the task (e.g. fixing a pipe as part of operation and maintenance). In overcoming data accessibility issues, existing research (Gao and Pishdad-Bozorgi, 2019; Mell and Grance, 2011) highlighted the need to have effective authorisation of access to data in place, however, this becomes complex when exchanging large volumes of data between multiple stakeholders.

Thus, this research supported highlighting the need to focus on process-related complexities, and how it can impact cybersecurity related considerations. From a people perspective, the literature sheds light on the probability of information loss resulting from the poor handling and management of digital information, which heighten the risk of unauthorised access to the data and the compromise of information confidentiality (Mantha, 2020). Also, reluctance towards the digital ways of working brought by BIM further affects the organisational approach towards developing knowledge, skills and awareness of working with digital tools in a BIM enabled facilities management (Akbarieh *et al.*, 2020). Hence, poor interaction of people and technology incurs opportunities for malicious cyber intrusions which inherently compromise the security of digital data in BIM project (Doneda and Almeida, 2015). The aforementioned factors will inherently result in an increased vulnerability towards cybersecurity attacks, targeting the integrity, availability and confidentiality of information, using the weak points in an organisational structure (Salminen, 2019; Sherman *et al.*, 2017). Therefore, it can be realised that process and people compose inevitable components when considering cybersecurity-related considerations in the built environment. Findings of this paper have revealed that with the increased number of stakeholders involved, this becomes more critical during post-occupancy phase where volume of information and the processes in-place to handle it can become complex.

7.2 Cybersecurity for BIM enabled FM: what is missing?

For tackling the issue of cybersecurity within digitalised organisations, such as BIM enabled facilities management, technological solutions are commonly used to protect the digital data from malicious cyber-attacks. Amongst the available technological solutions, block chain is a technology that allows encrypted and secure access to a system (Nofer *et al.*, 2017). Using block chain technology could be useful to decrease cyber risks as it reduces the need for third parties who facilitate digital collaboration between multiple stakeholders (Turk and Klinc, 2017). Therefore, it overcomes some of the cybersecurity issues that might affect the digital collaboration environment allowing for a more secure environment, especially in the case of an increased number of users. The technology also offers better defence when compared to other methods in the case of service providers and securing data (Blumzon and Pănescu, 2020; Li *et al.*, 2020). However, block chain like any other technology is vulnerable to the ever-advancing cybersecurity attack methods (Boyes, 2014a; Minoli *et al.*, 2017). This depends on the platform on which it is operating, which would result in heightened vulnerability to cyber infringements (Boxall, 2015; Portal, 2020). As block chain is mainly concerned with the asset management task area of a BIM-FM organisation, sole dependency on it to provide sufficient protection against cyber infringements inherently hinders the significance of cybersecurity in other task areas, including operations and maintenance, as well as space management. Therefore, it is recommended that organisations should invest in strategic cybersecurity management plans to enable technological excellence that allow optimum management of data security within digitalised working environments. Thus, developing a cybersecurity aware culture within a BIM enabled facilities management organisation would assist with increasing investments in this area. Hence, it is critical for the BIM enabled facilities management organisations to move towards a more proactive approach towards the management of cybersecurity risks.

7.3 Risk matrix to encompass cybersecurity risks for BIM enabled FM

Facilities management which is BIM enabled entails a common data environment that accommodates all information regarding the facility and the stakeholders involved. The as-built info-graphic information of the facility include details of the devices, installations, fittings as well as the detailed 3D model of various elements incorporated into the building. Hence, the implications of a cyber-attack to BIM enabled facilities management can impose a variety of threats to the facility. The common data environments used as a communication and collaboration platform also store personal data, financial information and intellectual property. Hence, malicious access to such information could also expose the facilities management organisations to reputational and financial loss (MSRC, 2019; Rogers, and Choi, 2018).

Furthermore, many buildings are facilitated with IoT devices and systems that are connected to the internet, and networks which enable real-time management and control over the building. Hence, intrusion into the systems can further allow remote control of these smart systems and lead to disruption in the facility's operations through device disablement (World, 2020). To further exemplify, information regarding the devices fitted inside a building, or access to the control systems could enable a fire alarm disablement, or CCTV disablement in favour of a planned physical attack (i.e. theft, destruction). This can in turn have health and safety implications for the occupants, leading to terror attacks and extortion opportunities (Boyes, 2015a; Weiss and Jankauskas, 2019).

[Table 2 here]

Table 2 presents a holistic view of the cybersecurity risks within various task areas of a BIM enabled facilities management organisation. It demonstrates the facilities management tasks in three key task areas of asset management, space management and operations and maintenance (Atkin & Brooks, 2015; Ebinger and Madritsch, 2012; Patacas *et al.*, 2015; Volk *et al.*, 2014). The review of the literature for BIM enabled facilities management indicated that the underpinning reason for adopting BIM is commonly related to the availability and accessibility of real-time information about the facility, which leads to an enhanced capability and optimised working processes (Abdelmohsen *et al.*, 2011; Akcamete *et al.*, 2011; Azhar *et al.*, 2009; British Institue of Facilities Management, 2012; Choi *et al.*, 2008; Group, 2013; Gu *et al.*, 2008; Keady, 2013; Ku and Taiebat, 2011; Reddy, 2011; Schade *et al.*, 2011). Therefore, this study presents the impact of a cybersecurity breach, on the benefits of BIM in various task areas of facilities management. This was approached based on the three aspects of the cybersecurity triad: confidentiality, integrity and availability of information. The review of the literature on cybersecurity within the built environment demonstrated a number of cybersecurity threats, including: theft of intellectual property; unauthorised access to confidential information; tampering with a facility's information; unauthorised access to systems in facilities; physical security breaches (e.g. unauthorised entry, burglary, terror), and harm to health and safety of occupants as a result. For instance, in the case of an unauthorised access to the BIM data, malicious tampering with information causes financial loss to the facilities management organisation by leading to misinformed decision making. Tampering with digital information can potentially disrupt functionality and result in operational disruption, or in some cases, harm to health and safety of personnel (Analytics, 2017; Ghosh *et al.*, 2019; MSRC, 2019; Parn and Edwards, 2019; Rogers and Choi, 2018; World, 2020). Hence, the risk matrix showcased the criticality of cyber risk impact in FM, with the aim of raising awareness amongst the FM professionals; and to encourage a proactive approach towards the development of a strategy to tackle the issue of cybersecurity, taking into consideration the role of people and processes in excelling the cybersecurity profile of a BIM enabled facilities management organisation.

8. Conclusion

This paper presents a holistic view of the issue of cybersecurity within a BIM enabled facilities management organisation. It discussed the cyber risks associated with the use of BIM in FM, and its cyber and physical implications on the facilities and their managing organisations.

The review of the literature illustrated a heightened risk of cybersecurity breach, due to the recent digital advancements in the built environment. The presence of IoT devices in buildings, coupled with building management systems, and their connections to BIM has created a golden thread of information that is desirable to those with malicious intentions of gaining unauthorised access to facilities or facilities management data. This paper draws attention to the criticality of cyber risk issues and their drastic impact on facilities and organisations. The conceptual BIM enabled FM specific cyber risk matrix is presented to serve as a trigger to industry and academia, for a shift of focus on the people and process aspects of cybersecurity of BIM in FM. Therefore, the future application and implementation of BIM in FM would be encouraged to invest in the enhancement of cybersecurity management capabilities, by integrating knowledge of cybersecurity risks associated with various tasks within a BIM enabled facilities management.

The proposed cybersecurity risk matrix is a baseline for future research in this matter. As this work was seldom based on secondary data, future studies can investigate the cybersecurity matrix in real life case studies across the FM industry. At this moment in time, the application of BIM in facilities management is still at its infancy. Hence, resources discussing the challenges associated with BIM implementation in FM are very limited and scarce. Therefore, with the rise of BIM maturity in FM, access to empirical data would be more feasible for future research, to investigate the challenges associated with BIM projects in FM, and in particular, cybersecurity challenges.

References

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*.

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.

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

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., Liu, X., Akinci, B. and Garrett Jr, J.H. (2011), “Integrating and Visualizing Maintenance and Repair Work Orders In BIM: Lessons Learned From A Prototype”, *International Conference On Construction Applications of Virtual Reality*.

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.

Alguliyev, R., Imamverdiyev, Y. and Sukhostat, L. (2018), “Cyber-physical systems and their security issues”, *Computers in Industry*, available at:https://doi.org/10.1016/j.compind.2018.04.017.

Alkasisbeh, M.R. and Abudayyeh, O. (2018), “Building asset management system: A performance evaluation approach”, *IISE Annual Conference and Expo 2018*.

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.

El Ammari, K. and Hammad, A. (2019), “Remote interactive collaboration in facilities management using BIM-based mixed reality”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2019.102940.

Analytics, D.D. and. (2017), *SmartMarket Brief: Leading the Future of Building Connecting Teams*.

ANSI. (2007), *Security for Industrial Automation and Control Systems; Part 1: Terminology, Concepts, and Models*, available at: https://web.archive.org/web/20110312 111418/www.isa.org/Template.cfm?Section=Shop_ISA&Template=%252FEcommerce %25 2FProductDisplay.cfm&Productid=9661.

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.

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).

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*.

Atkin, B., & Brooks, A. (2015), *Total Facility Management*, John Wiley & Sons.

Azhar, S., Brown, J. and Farooqui, R. (2009), "BIM-based Sustainability Analysis : An Evaluation of Building Performance Analysis Software", *Proceedings of the 45th ASC Annual Conference*.

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.

Barrett, P. and Baldry, D. (2003), *Facilities Management: Towards Best Practice*, *Facilities Management*.

Becerik-Gerber, B., Jazizadeh, F., Li, N. and Calis, G. (2012), "Application Areas and Data Requirements for BIM-Enabled Facilities Management", *Journal of Construction Engineering and Management*, Vol. 138 No. 3, pp. 431–442.

Becker, F. and Steele, F. (1990), "The total workplace", *Facilities*, available at:https://doi.org/10.1108/eum0000000002099.

Blumzon, C.F.I. and Pănescu, A.T. (2020), "Data Storage", *Handbook of Experimental Pharmacology*, available at:https://doi.org/10.1007/164_2019_288.

Boxall, E. (2015), "Common Data Environment (CDE): What you need to know for starters."

Boyes, H. (2014a), *Building Information Modelling (BIM): Addressing the Cyber Security Issues*, London.

Boyes, H. (2014b), *Cyber Security Attributes for Critical Infrastructure Systems*, available at: http://cybersecurity-review.com/editions/ cyber-security-review-summer-2014-edition.

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), "Security, privacy, and the built environment", *IT Professional*, available at:https://doi.org/10.1109/MITP.2015.49.

Bradley, A., Li, H., Lark, R. and Dunn, S. (2016), "BIM for infrastructure: An overall review and constructor perspective", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2016.08.019.

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.

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*.

Bryde, D., Broquetas, M. and Volm, J.M. (2013), "The project benefits of building information modelling (BIM)", *International Journal of Project Management*, available at:https://doi.org/10.1016/j.ijproman.2012.12.001.

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.

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.

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.

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, W., Chen, K., Cheng, J.C.P., Wang, Q. and Gan, V.J.L. (2018), “BIM-based framework for automatic scheduling of facility maintenance work orders”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2018.03.007.

Choi, Y., Kang, D., Chae, H. and Kim, K. (2008), “An enterprise architecture framework for collaboration of virtual enterprise chains”, *International Journal of Advanced Manufacturing Technology*, available at:https://doi.org/10.1007/s00170-006-0789-7.

Codinhoto, R., Kiviniemi, A., Kemmer, S., Esseit, U.M., Donato, V. and Tonso, L.G. (2013), “Research Report 2 - BIM - FM - Manchester Town Hall Complex. Manchester City Council”, p. 92.

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.

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.

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.

Dunn Cavelty, M. (2005), “A Comparative Analysis of Cybersecurity Initiatives Worldwide”, *WSIS Thematic Meeting on Cybersecurity*.

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.

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.

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.

Ghaffarianhoseini, A., Tookey, J., Ghaffarianhoseini, A., Naismith, N., Azhar, S., Efimova, O. and Raahemifar, K. (2017), “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.

Glantz, C., Somasundaram, S., Mylrea, M., Underhill, R., & Nicholls, A. (2016), *Evaluating the Maturity of Cybersecurity Programs for Building Control Systems*.

Griffin, P.H. (2019), “Advances in Human Factors in Cybersecurity”, *Advances in Intelligent Systems and Computing*.

Group, B.T. (2013), “Employer’s Information Requirements: Core Content and Guidance Notes”.

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*.

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.

Hetemi, E., Ordieres-Meré, J. and Nuur, C. (2020), “An institutional approach to digitalization in sustainability-oriented infrastructure projects: The limits of the building information model”, *Sustainability (Switzerland)*, Vol. 12 No. 9, available at:https://doi.org/10.3390/su12093893.

Hjelseth, E. (2010), “Exchange of relevant information in BIM objects defined by the role- and life-cycle information model”, *Architectural Engineering and Design Management*, available at:https://doi.org/10.3763/aedm.2010.IDDS5.

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*, available at:https://doi.org/10.1088/1757-899X/869/2/022032.

Hong, Y., Hammad, A.W.A. and Akbarnezhad, A. (2019), “Forecasting the net costs to organisations of building information modelling (BIM) implementation at different levels of development (LOD)", *Journal of Information Technology in Construction*, available at:https://doi.org/10.36680/J.ITCON.2019.033.

Hooper, M. (2015), "Automated model progression scheduling using level of development", *Construction Innovation*, available at:https://doi.org/10.1108/CI-09-2014-0048.

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.

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.

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.

Kabanda, G. (2018), "A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations", *Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations. AJMECS*.

Kadefors, A. (2008), "Contracting in FM: collaboration, coordination and control", *Journal of Facilities Management*, available at:https://doi.org/10.1108/14725960810885943.

Kang, T.W. and Choi, H.S. (2015), "BIM perspective definition metadata for interworking facility management data", *Advanced Engineering Informatics*, available at:https://doi.org/10.1016/j.aei.2015.09.004.

Kassem, M., Kelly, G., Dawood, N., Serginson, M. and Lockley, S. (2015), "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.

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. (2013), "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.

Kensek, K. (2015), "BIM guidelines inform facilities management databases: A Case Study over Time", *Buildings*, Vol. 5 No. 3, pp. 899–916.

Khajuria, S., Sørensen, L. and Skouby, K.E. (2017), *Cybersecurity and Privacy - Bridging the Gap., Cybersecurity and Privacy*.

Kim, K., Kim, H., Kim, W., Kim, C., Kim, J. and Yu, J. (2018), "Integration of ifc objects and facility management work information using Semantic Web", *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2017.12.019.

King, N., Cassell, C. and Symon, G. (2004), “Using templates in the thematic analysis of texts”, *Essential Guide to Qualitative Methods in Organizational Research*.

Koch, C., Neges, M., König, M. and Abramovici, M. (2014), “Natural markers for augmented reality-based indoor navigation and facility maintenance”, *Automation in Construction*, available at:https://doi.org/10.1016/j.autcon.2014.08.009.

Korpela, J., Miettinen, R., Salmikivi, T. and Ihalainen, J. (2015), “The challenges and potentials of utilizing building information modelling in facility management: the case of the Center for Properties and Facilities of the University of Helsinki”, *Construction Management and Economics*, available at:https://doi.org/10.1080/01446193.2015.1016540.

Ku, K. and Taiebat, M. (2011), “BIM experiences and expectations: The constructors’ perspective”, *International Journal of Construction Education and Research*, available at:https://doi.org/10.1080/15578771.2010.544155.

Lavy, S. and Jawadekar, S. (2014), “A Case Study of Using BIM and COBie for Facility Management”, *International Journal of Facility Management*.

Lea, G., Ganah, A., Goulding, J. and Ainsworth, N. (2015), “Identification and analysis of UK and US BIM standards to aid collaboration”, *Building Information Modelling (BIM) in Design, Construction and Operations*, available at:https://doi.org/10.2495/bim150411.

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.

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.

Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q. (2020), “A survey on the security of blockchain systems”, *Future Generation Computer Systems*, available at:https://doi.org/10.1016/j.future.2017.08.020.

Lin, S., Gao, J., Koronios, A. and Chanana, V. (2007), “Developing a data quality framework for asset management in engineering organisations”, *International Journal of Information Quality*, available at:https://doi.org/10.1504/IJIQ.2007.013378.

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.

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.

Mandhar, M. and Mandhar, M. (2013), “BIMing The Architectural Curricula-Integrating Building Information Modelling (BIM) in Architectural Education International Journal of Architecture IJA © I A E M E”, *International Journal of Architecture (IJA)*.

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.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.

Marinos, L. (2013), "ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats", *European Union Agency for Network and Information Security*.

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.

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.

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*.

McGraw Hill Construction. (2012), *The Business Value of BIM in North America, SmartMarket Report*.

Mell, P. and Grance, T. (2011), "The NIST definition of cloud computing - SP 800-145", *NIST Special Publication*.

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.

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*.

MSRC. (2019), "Corporate IoT – a path to intrusion", available at: https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion (accessed 5 October 2020).

Naghshbandi, S.N. (2016), "BIM for Facility Management: Challenges and Research Gaps", *Civil Engineering Journal*, available at:https://doi.org/10.28991/cej-2016-00000067.

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.

Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017), "Blockchain", *Business and Information Systems Engineering*, available at:https://doi.org/10.1007/s12599-017-0467-3.

Nye, J. (2018), "How Will New Cybersecurity Norms Develop?", *Project Syndicate*.

Parn, E.A. and Edwards, D. (2019), "Cyber threats confronting the digital built environment", *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.

Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X. and Xie, F. (2013), “Cyber-physical system risk assessment”, *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, available at:https://doi.org/10.1109/IIH-MSP.2013.116.

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.

Pocock, D., Shetty, N., Hayes, A. and Watts, J. (2014), “Leveraging the relationship between BIM and asset management”, *Infrastructure Asset Management*, Thomas Telford Ltd, Vol. 1 No. 1, pp. 5–7.

Pop, F., Dobre, C., Cristea, V., Bessis, N., Xhafa, F. and Barolli, L. (2015), “Deadline scheduling for aperiodic tasks in inter-Cloud environments: a new approach to resource management”, *Journal of Supercomputing*, available at:https://doi.org/10.1007/s11227-014-1285-8.

Portal, B. (2020), “BIM - Digital Information Management to Improve Infrastructure Delivery and Performance”, available at: https://bimportal.scottishfuturestrust.org.uk/page/new-international-bim-standards (accessed 1 September 2020).

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.

Reddy, K.P. (2011), *BIM for Building Owners and Developers*, *BIM for Building Owners and Developers*, available at:https://doi.org/10.1002/9781119572602.

Rogers, Z. and Choi, T. (2018), “Purchasing Managers Have a Lead Role to Play in Cyber Defense”, available at: https://hbr.org/2018/07/purchasing-https://hbr.org/2018/07/purchasing-managers-have-a-lead-role-to-play-in-cyber-defensemanagers-have-a-lead-role-to-play-in-cyber-defense (accessed 5 October 2020).

Ryan, D.J. (2017), “Engineering sustainable critical infrastructures”, *International Journal of Critical Infrastructure Protection*, Vol. 17, pp. 28–29.

Sackey, E., Tuuli, M.M. and Dainty, A. (2013), “Bim Implementation : From Capability Maturity Models To Implementation Strategy”, *Sustainable Building Conference 2013*.

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.

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.

Services, A.W. (2018), “Types of Cloud Computing”, available at: https://aws.amazon.com/types-of-cloud-computing/.

Sharma, A., Gandhi, R.A., Mahoney, W., Sousan, W. and Zhu, Q. (2010), “Building a social dimensional threat model from current and historic events of cyber attacks”, *Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust*, available at:https://doi.org/10.1109/SocialCom.2010.145.

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.

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*.

Sridarran, P. and Fernando, N.G. (2016), “Change management framework to enable sustainable outsourcing of facilities management services”, *Built Environment Project and Asset Management*, available at:https://doi.org/10.1108/BEPAM-08-2014-0041.

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.

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*.

Szyliowicz, J.S. and Zamparini, L. (2014), “Maritime security: Issues and challenges”, *Maritime Transport Security: Issues, Challenges and National Policies*, available at:https://doi.org/10.4337/9781781954973.00008.

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.

Terreno, S., Anumba, C.J. and Dubler, C. (2016), “BIM-Based Management of Building Operations”, *Construction Research Congress 2016: Old and New Construction Technologies Converge in Historic San Juan - Proceedings of the 2016 Construction Research Congress, CRC 2016*, No. May, pp. 1855–1865.

Turk, Ž. and Klinc, R. (2017), “Potentials of Blockchain Technology for Construction

Management", *Procedia Engineering*, available at:https://doi.org/10.1016/j.proeng.2017.08.052.

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 & …*.

Weiss, M. and Jankauskas, V. (2019), "Securing cyberspace: how states design governance arrangements", *Governance*, available at:https://doi.org/10.1111/gove.12368.

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.

World, I. (2020), "Facility Managers Guide to Building Systems and Cybersecurity", available at: https://iiot-world.com/ics-security/cybersecurity/facility-managers-guide-to-building-systems-and-cybersecurity/ Cybersecurity, ICS Security (accessed 5 October 2020).

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.

Yu, K., Froese, T. and Grobler, F. (2000), "Development framework for data models for computer-integrated facilities management", *Automation in Construction*, available at:https://doi.org/10.1016/S0926-5805(99)00002-3.

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.