Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems

Yussuf Ahmed Syed Naqvi Mark Josephs
School of Computing and Digital Technology, Birmingham City University, UK

***Abstract*—Cybersecurity incidents are on the rise in the healthcare sector and it is becoming a growing concern for the senior executives. The attack surface is expanding due to the large number of connected medical devices and the proliferation of portable devices such as smart phones, tablets and USB devices. In this paper, we will discuss some of the security challenges facing this sector and propose a set of cybersecurity metrics that could be used to enhance the protection of the IT systems.**

***Index Terms*—Cybersecurity, Healthcare, Interconnected devices, Network security, Security metrics, Medical devices, Infrastructure, Security culture, Ransomware**

I. Introduction

The need for interconnected devices in healthcare settings has become a necessity given the number of clinicians and other healthcare professionals who need access to the patient information in order to deliver a good quality patient care and to avoid duplication. While Interconnecting these devices brings lots of benefits, it also introduces security issues that could compromise the privacy and integrity of the data [1]. Security metrics can provide organisations with a mean to measure and understand the security status of their systems given attackers are always looking for the weakest link [2].

Clinicians and other healthcare professionals might not see security from the same perspective as IT professionals and are mainly driven by the need to deliver excellent patient care [3]. Security metrics can help stakeholders to learn about the insight and trends in their organisation and to measure how the organisation is performing against their peers in the industry [4]. The healthcare sector had numerous security breaches over the last few years and the trend has been increasing. According to a recent Verizon data report, the number of security breaches in the healthcare sector has substantially increased from the previous year and 85 percent of the malware targeting this industry is Ransomware [5]. A similar report by the SecuritySecorecard found the lack of security awareness training among staff in the healthcare sector which is putting the entire infrastructure at risk [6]. The healthcare sector faces some unique challenges given the vast amount of sensitive data they hold, the ageing infrastructure especially in public hospitals and complexity due to the large number of endpoints [7]. The industry as a whole also lags behind in security compared to the other sectors and must improve their security in order to protect their key assets [8].

The reminder of this paper is organised as follows: Section II covers healthcare exposure to cyber threats. Section III presents security metrics including the proposed metrics categorisations and the relevant sub-metrics. Finally, Section IV concludes the paper with a summary and future work.

II. Healthcare exposure to cyber threats

The biggest threat to the healthcare sector is attacks on the healthcare infrastructure, services and medical devices which can compromise the safety of patients [9]. Availability and correctness are key factors that are critical to the delivery of a healthcare service but these are threatened by hackers who are always looking for vulnerable systems to target. Hackers are attracted to the healthcare sector due to the value of the sensitive data they hold and ease of the target [10].

The healthcare sector shares most of the threat vectors with other industries however the impact of a compromise is much higher given it involves the safety of patients. Priya et al. [11] described some of the security attacks that are targeted at healthcare systems and the challenges they pose to the security, integrity and availability of sensitive data. The authors characterised the security attacks into three phases which are: the data gathering phase, network gathering phase and Storage phase. There are a large number of wireless devices connected to the hospital networks but while these devices help clinicians and other healthcare professionals to deliver effective patient care, they also increase the attacks surface [12].

Ransomware is a category of malware that encrypts user data to extort money and is often referred to a digital form of blackmail [13], [14]. Ransomware is one of the most popular attacks that has widely been used against the healthcare sector in the recent years. The WannaCry incident which affected the UK National Health Service showed the impact of such attacks on a critical infrastructure. WannaCry exploited a known Server Message Block(SMB) vulnerability [15]. Ransomware attackers are usually interested in extorting money from their victims by encrypting their files and affecting availability of the data but a recent ransomware attack on the offices of a Podiatric specialist was reported to have corrupted or modified 24000 patient records [16]. Attackers usually deceive innocent victims by sending them links to click which then downloads the Ransomware malware to their systems but they also use methods such as drive-by freeware [17]. Ransomware has become the preferred choice for cybercriminals due to its ease of use, availability of the Ransomware toolkits and decentralised cryptocurrencies such as Bitcoin [18], [19]. In the case of UK NHS, the WannaCry ransomware spread quickly from one system to another affecting over 50,000 machines at its peak [20]. In the following sub-sections, we

will cover some the reasons why the healthcare sector is susceptible to cyberattacks.

A. Ageing infrastructure

The threat landscape is constantly changing and organisations have to be well prepared to maintain business continuity if their critical services are affected by cyberattacks but the healthcare sector and especially public hospitals are known to be using legacy systems which are vulnerable to cyberattacks. The WannaCry incident which almost brought part of the UK National Health Service to standstill is one example where unsupported systems introduced threats to the organisation. WannaCry was the largest Ransomware ever seen having affected 11 countries in just three hours [21]. Ransomware attacks continued to target the healthcare sector while Phishing and misconfiguration resulted in a large number security breaches [22]. Patch management is one area that is not fully implemented due to the ageing systems which are no longer supported by the vendors or for fear of the updates breaking this critical systems [23]. Privacy and security is a major concern in health institutions due to the vast amount of sensitive data they hold [24]. Several authors have discussed the adaptation of Cloud computing in Healthcare to overcome some of the challenges posed by the ageing infrastructure however Cloud computing has it own privacy and security issues which is why some providers are hesitant to embrace the Cloud paradigm [25], [26], [27], [28].

B. Medical devices

Medical devices that were previously not connected to the internet are nowadays online to ease data sharing amongst clinicians and to provide result promptly. However, these medical devices will also inevitably introduce vulnerabilities to the network and increase the attack surface [29]. The manufacturers of these medical devices did not usually have security in mind when they were designed. Vulnerable medical devices could be an entry point for hackers to attack the hospital network [30] .The presence of malware on computer systems can significantly affect the security of the medical devices. These days medical devices are connected to computers to allow health professionals to share medical diagnosis such as ultrasound results instantly but these can mean malware being transferred from one system and another and eventually to the wider hospital network [31].

The US Food and Drug Administration (FDA) provided guidelines for hospital and healthcare networks in relation to securing medical devices and healthcare networks. Measures such as restricting unauthorised access for both medical devices and hospital networks, implementing network monitoring to detect intrusions, cyber hygiene, capability to set medical devices to fails-safe and sharing medical devices vulnerabilities with manufacturers were proposed [32]. The FDA also released a final post market management of medical devices during the whole lifecycle and stresses the need to perform risk assessments to determine exploitability and impact on patient health and evaluate risk to patient safety. [33]

The current Common Vulnerability Scoring System(CVSS) does not often take clinical environments into account and a common framework for security and safety of this devices will go along way in addressing some of these challenges [30]. The ISO 80001 standards on the application of risk management for IT-networks incorporating medical devices provides guidance on security and risk management for healthcare organisations but its effectiveness in dealing with modern and complex cybersecurity challenges is unknown [34].

Compromised medical devices do not just introduce risks to the network and they can also have serious effect on patient's health [35]. For example a misconfiguration of medical devices such as X-ray machines by attackers could expose patients to serious risks [36]. Similarly there are a large number of Internet of Things (IOT) smart devices such as insulin pumps that could be compromised by attackers given they connect to wireless networks to upload to their data to the network. A survey by Deloitte which involved 17 hospitals in the Netherlands reported that there was an increase in the number of medical devices that were interconnected and more than half of the participants reported their medical devices were infected with viruses [31]. Wellington et al. [37] discussed common cyber attack methods against medical devices and categorised them into 3 categories: Unauthorised access, DoS/DDoS attacks and Malware attacks.

C. Security culture

Security awareness training is often regarded as one the best security measures given humans could be susceptible to social engineering and become the weakest link on the network for attackers to exploit. Clinicians and other healthcare professionals are often driven by the need to deliver excellent patient care and security controls such as strong passwords could be been as a hinderance rather than a security measure hence why password sharing was found to be prevalent in the healthcare sector [3]. Sharing passwords not only introduces security risks but it can have serious impact on patient safety due to the possibility of a mixup and subsequent doctors updating the wrong patient information or using a medical device with a customised settings for a previous patient by mistake [38]. The healthcare sector will need to employ senior security officers to oversee the Cybersecurity side of the business including the user awareness training. The UK National Health Service recently created a new post of Chief Information Security Officer (CISO) following on the lessons learnt from the WannaCry Ransomware attacks [39].

D. Legal and regulatory compliance

Hospital executives must ensure they have appropriate security measures in place to protect the data they hold. Such security measures include encryption, data sanitisation and appropriate access control mechanisms in order to restrict access to only those who are authorised. The senior managers should also educate their employees on the consequences of

accessing patients information without any valid reason and appropriate actions should be taken against those who misuse their privileges. A healthcare administrator was recently fined in the UK for accessing patients records without a valid reason [40].

There are several laws and regulations that protect the privacy and confidentiality of patients. For example, in the UK along with the General Data Protection Regulation(GDPR) compliance requirement, there is also the Caldicott report which sets out six principles for organisations to follow in order to protect the privacy and confidentiality of their patients [41]. The National Data Guardian (NDG) challenges healthcare organisation to ensure the data of their patients is securely protected and properly used [42]. In the US the Health Insurance Portability and Accountability Act (HIPAA) regulates the security and privacy of data held by healthcare providers [43].

E. Summary

In this section, we described some of the security challenges facing the healthcare sector and the motivations of the cybercriminals. We mentioned some of the reasons why healthcare institutions are susceptible to cyberattacks including the vast number legacy systems, softness of the target and the value of the data they hold.

In the next section, we will provide a brief overview of security metrics and present metrics that could be used to protect the healthcare IT systems. The proposed metrics could also be used in any other industry however these metrics will contribute immensely to improving the security of healthcare IT systems given this sector's susceptibility to cyberattacks and the risk such attacks pose to patient safety. The security of these systems will need to be monitored in a more meaningful manners and quantifying these metrics will assist IT security professional to put in place the right controls for mitigating potential risks.

The proposed security metric categories could also be quantified to help senior managers make informed decision including investments on security measures. It is worth noting that the SMB vulnerability exploited by WannaCry was known for three months and having security metrics such as percentage of systems with known vulnerabilities that have not be patched, could have been very useful and maybe resulted in preemptive actions being taken to avoid the risk.

III. Security Metrics

Security metrics has been gaining interest from researchers in academia and the industry to help quantify security measurements and assist with decision making. According to a recent report by Thycotic, most organisation are failing to implement cybersecurity metrics and therefore unable to evaluate and track the effectiveness and performance of their security mechanisms [44]. Several authors have published work on security metrics [45], [46], [47], [48], [49], [50], [51] but these were mainly targeted at organisational level and not captured in the context of healthcare IT systems.

Ahmed et al. [52] conducted a review of security metrics and proposed a reference architecture for aggregating the security of an enterprise network. Jafari et al. [53] discussed security metrics in e-health and proposed an approach that consists of five elements; technology maturity analysis, threat analysis and modelling, requirements establishment, policies and mechanisms, and system behaviour but the method for developing the metrics was not described.

Liu et al. [54] focused on the implementation of IPSec to protect the confidentiality and integrity of sensitive patient data from cyber threats and demonstrated how to implement the controls. Abie and Balasingham [55] proposed a risk based adaptive security framework for IOT in eHealth that allows systems to learn and adopt to changes in the environments by anticipating threats. Savola et. [4] performed risk analysis on an e-health self-care system and quantified the metrics using risk assessments technique based on severity and impact. Muthukrishnan et al. [56] proposed a quantitative and qualitative metrics maturity method based on a scorecard.

In the following sub-sections, we present some security metrics that could be used to address the cybersecurity challenges discussed in the previous section and describe how these metrics could be used to improve the security of the IT systems.

We believe the metric categories we are proposing have a wider coverage and could be used to measure and improve the security status of the IT systems including interconnected devices. Although these metrics could be applied to any organisation, we believe their positive impact will be felt more in the healthcare sector where the attack surface is much larger due the vast number of legacy systems, interconnected medical devices, complexity of the endpoints, security culture and the high value of the data they hold.

In fig. 1, we categorised the security metrics into eight groups which are: Indicators of compromise, indicators of attacks, resilience, red and blue teaming, vulnerability assessment, intelligence driven defence, risk assessment and penetration testing. In the following sub-sections, we will describe each of the categories in more detail.

A. Indicators Of Compromise based metrics (IOC)

Indicators of compromise are information that can used to identify malicious activities that has taken place on a system or network [57]. The information relating to these security breaches can be used to prevent similar attacks in the future. Monitoring for indicators of compromise can help organisations to quickly detect incidents that may have been missed by the monitoring tools.

Incidents such as malware attacks often take along time before they are detected by the affected organisations or by the security community and by that time lots of sensitive data may have been stolen [58]. Once the IOCs are detected and shared, organisation could act on these indictors to mitigate the risks and prevent future attacks. Sharing cybersecurity intelligence such as Indictors of compromise could allow organisations to defend against sophisticated cyberattacks [59]. For example,

in the case of WannaCry, there were three IOCs which were detected following on the first wave of attacks. One of this was a dropper which contained the ransomware and used to run it while the other two were encryption plug-ins [60].

Data relating to indicators of compromise such as artefacts that are left after malware executions could be obtained from the logs files. Monitoring tools such as anti-virus systems are known to use indictors of compromise to block malware. Tounsi at al. [61] categorised indicators of compromise into Network-based indicator (IP addresses, Urls and Domain names), Host-based indicators (malware names, signature and registry keys) and email-based indicators (source IP, header, attacked link).

There are free tools such as Redline from FireEye which can be used to perform indicators of compromise analysis on systems [62]. Other web-based tools such as IOC Bucket [63] and IOC editor [64] can be used to share, research, create and edit IOCs. Catakoglu et al. [65] proposed an automated technique for collecting indicators of compromise from webpages in a honeypot setup.

Metrics based on IOC could assist IT professionals including those in healthcare to learn more about the security threats affecting their systems and to use the lessons learnt to prevent future attacks. In the next points. we will mention some useful metrics relating to IOC and point out how they could be used by security professionals to enhance the protection of their systems.

- Volume of outbound traffic. unusual increase in outgoing traffic could be a sign of data exfiltration [66]. Organisations have a responsibility to protect their sensitive data and any breach is likely to attract attention from the government bodies with responsibilities for enforcing the data protection laws such as GDPR.
  The large volume of personal data held by the healthcare providers is one the reasons why the cybercriminals target this sector. Using this indicator of compromise will allow healthcare IT professionals to look for incidents that may have been missed by the security monitoring tools. It is paramount that IT professional correlate log data from affected systems and the other network monitoring tools to determine exactly what happened including the type of malware.
- Volume and number of IP addresses connecting to your network from outside of your geographical area. Successful logins from outside your region could be an indication of a security breach. Given the complexity of the endpoints and the legacy systems that are still in use in the healthcare institutions especially in public hospitals, there are more chances of breaches not being detected compared to other sectors such as the financial sector. Hunting for indictors of compromise such as external IP addresses from outside of your normal geographical area could allow the IT security professionals to find out whether successful login was established and to investigate the incidents further.
- Number of simultaneous logins by the same user from different locations that has not been detected by the network security tools. This could be an indication of sophisticated attacks that bypassed the security controls. Investigating this IOC will help IT security professional to determine the chain of events that led to this breach and to fine tune their security controls to help detect or prevent similar attacks in the future.
- Percentage of traffic from onion router that was not detected by the network monitoring tools. This metrics can be used to test the effectiveness of your security control [67]. Cybercriminal are known to disguise their identity by moving data across multiple Tor nodes making it difficult to trace back their activity. IT security teams should ensure this metrics is monitored and appropriate security measures taken to mitigate risk associated with it.
- Number of unknown accounts with elevated privileges found on compromised systems. This may be an indication that the systems were compromised and that the attacker performed escalation of privileges to take ownership and create backdoors.

B. Indicators Of Attack Metrics

Indicator Of Attack (IOA) is a proactive security measure that could be used to reveal an attack that is taking place before the indicators of compromise become visible [68]. IOAs could help organisations to disrupt attackers before they exploit the systems by putting in place mitigating controls. For example, IOAs could be used to prevent attacks such as Phishing and ransomware which has become a popular attack vector targeted at healthcare providers. Implementing IOAs metrics such as those shown below, could help organisations to increase their proactive approaches and prevent attacks that could have otherwise compromised their systems.

- Lateral movements. This could indicate an attacker has gained access to the network and is moving from one vulnerable host to another until the goal is achieved [69]. Due to the complexity of the setup and number of interconnected devices in healthcare institutions, IT security professionals will need to monitor this metric to enable them to act promptly and implement corrective measures to disrupt such activity.
- High Bandwidth and increased outgoing traffic. This could be a sign of DDoS attack or data exfiltration [70]
- Number of hosts communicating with external networks on non-standard ports. This could be an indication of sophisticated attackers hiding their activities. An attacker could use non-standard port numbers to avoid detection by the security controls. Monitoring this metric could help security professionals to stop unauthorised connections and to update the secure measures.
- High number of failed authentication attempts. This could be an indication of an attacker attempting to gain access to your network using brute-force.

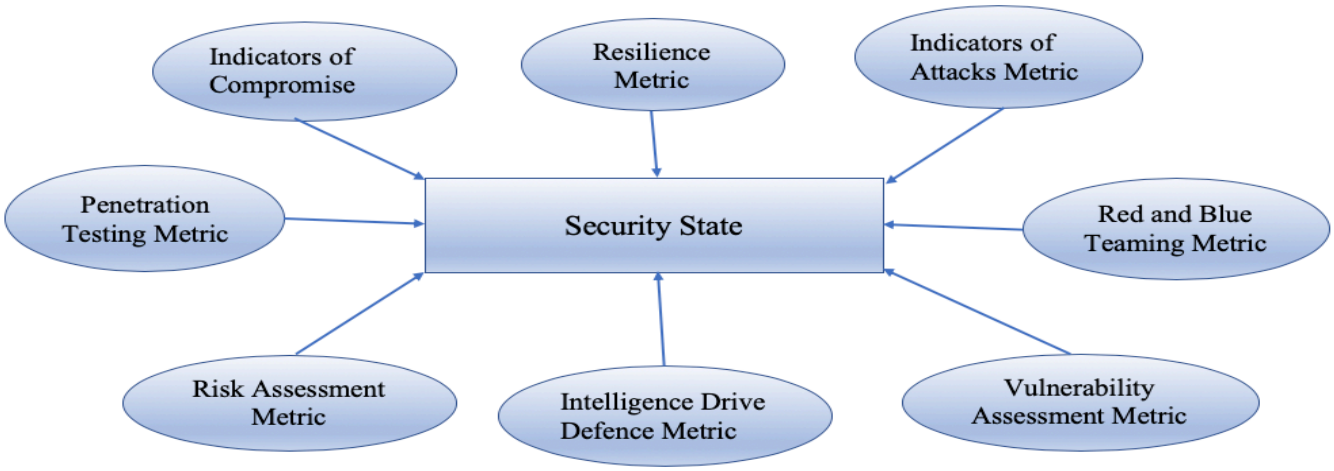

Fig. 1. Security Metrics

- Number of processes with high memory consumption. This could be an indication that malware is being executed. Malware usually runs on the memory and security professionals should investigate spikes in memory usage to determine whether malware execution is taking place.

C. Risk Assessment Metrics

Understanding what needs to be protected is the first step in the risk assessment process. Asset identification and classification will need to be performed in order direct resources to the most critical assets. The healthcare institutions hold lots of sensitive data relating to their patients and it is important for all assets to be accounted for and their impact on the business quantified. A risk register should be maintained and populated with risks that were identified along with any corrective measures taken and should be regularly updated. Organisation can use security metrics to maintain oversight on their risk management processes. Such metrics include:

- Percentage of risks with severe or critical rating. This will help to prioritise and direct resources to deal with the most urgent threats affecting the critical assets. The healthcare sector especially public hospitals have limited resources and monitoring this metrics will enable them to prioritise and deal with risks with highest severity.
- Percentage of key assets with no ownership assigned. Asset ownership is key to determining the right safeguards needed to protect these systems. Given the ever changing threat landscape and the presence of legacy systems in the healthcare sector, it is just a matter of time before such systems are compromised. Resuming services and invoking recovery plans for such systems depends on the assets owner if the system is to be restored with limited downtime. Organisations should ensure all assets have an owner.
- Percentage of assets that are monitored. This metric will help with monitoring the coverage and determine if gaps exist. Considering how critical some of these systems are to service delivery and their complexity in healthcare setting, efforts should be made to ensure coverage is maximised.

D. Penetration Testing Metric

Penetration testing is a method for detecting security vulnerabilities on a network and can involve simulated attacks [71]. Due to the costs involved, organisations have the tendency to perform penetration testing on quarterly or biannually basis but the threat landscape could change very quickly and make such tests redundant within a short period. To fill this gap, newer penetration testing tools that operate inside the network have been developed by companies. For example Firedrill developed the AttackIQ [72] which is a tool that performs automated testing to determine the enterprise security posture but these

tools are not yet widely adopted. Healthcare institutions have a large attack surface due to the vast number of endpoints and legacy systems. Performing regular penetration testing on these systems will enable the organisations to detect weaknesses and implement the necessary controls to prevent potential attacks. One way to maximise these tests is to use penetration testing metrics. Such metrics include but not limited to:

- Percentage of penetration tests that discovered high risks. This can indicate a measure of how well the existing security controls are performing including the detection capability of the vulnerability management tools.
- Penetration testing intervals. The threat landscape changes over time and increasing the frequency of testing will help organisations to uncover security risks and help prevent potential attacks. It can also be used to measure how well vulnerabilities detected in the previous tests were resolved.
- Penetration testing coverage. In healthcare settings, the coverage metric should include all critical systems such as medical devices and the infrastructure. Ideally, all assets should be covered.
- Mean Time To Fix (MTTF). This metrics will show the average time taken to fix the vulnerabilities that were identified during the penetration testing and also allow senior managers to measure the capability and average response times of the technical teams.

E. Vulnerability Assessment Metric

Vulnerability is a weakness on a system that could be exploited by a threat [73]. where possible organisations should be implementing automated vulnerability scanning tools to enable them to detect vulnerabilities more efficiently and in a consistent manner. System administrators should monitor and deal with the detected vulnerabilities promptly according their severity and impact. The vulnerability assessment tools are likely to detect large number of vulnerabilities in healthcare institutions such as public hospitals. One ways to maximise the effectiveness of the response is to use vulnerability metrics and such metrics include:

- Percentage of critical systems with known vulnerabilities that are not patched. This metric will help organisations to determine how well they are implementing their security patches. Systems with known vulnerabilities face a higher risks given this information is publicly available on the vulnerability databases. The SMB vulnerability which was exploited by the WannaCry ransomware is one example of known vulnerabilities which could have been prevented with a simple patch.
- Meantime To Detection (MTD). This metric will enable organisations to test how well vulnerabilities are detected including the effectiveness of their vulnerability management systems and other security controls.
- Exposure time. This is the duration between detection and application of the patch and could be used to measure how quickly the system administrators are applying patches. The earlier the patch is applied the better.

F. Red and Blue Teaming Metric

Red teaming is a simulated form of attack in which skilled teams attempt to penetrate the security defences and compromise the systems. Organisations usually employ the service of red teams in order to test the maturity of their security controls [74]. After the end of the red team assessment, organisations will have a list of attack vectors they are vulnerable to and corrective measures to mitigate such risks.

Red teams should be complemented with Blue teams whose role is to defend against the attacks and bolster the security defences. The purpose of a Blue team is to defend the organisation against both Red teams and real attackers [75]. Enlisting the service of Red teams can be expensive and organisations should try to maximise this potential to improve their security.

Red and Blue teams could also be used during the optimisation stages after new security programs are deployed. Organisations can use metrics to measure how well they are integrating the outcome from the Red team assessment to improve the strength of their security mechanisms. Such metrics include:

- Resources required to breach the security defences and compromise the systems. This will indicate how well the systems are protected and the layers of defence. The security defences should be strong enough withstand most attacks and the more resources required to break in the better the defence mechanisms.
- Skills and knowledge of the attackers. This metric can be used to determine the expertise and sophistication required to break into the systems and the information obtained from this metric could be used to increase the security strength.
- Profiling the attacker. System administrators could use honey-nets to build an overall picture of the attacker. This metric could be used to put in place mitigation controls and to beef the defensive capabilities.

G. Resilience Metric

Resilience is the ability for a system to adapt and continue to provide functionality in face of an attack [76]. The healthcare sector experienced vast number of targeted attacks which disrupted critical services as seen with the WannaCry attack on the UK National Health Service(NHS). Ransomware attacks such as WannaCry encrypts the files and make them unavailable to the users until a ransom is paid. Resilience will enable organisations to withstand adversarial attacks and to ensure continuity of critical services [77]. The following are some of the metrics that could be used to measure resilience in an organisation.

- Mean Time To Repair (MTTR). This metric will enable systems administrators to monitor how quickly they respond to incidents that disrupts availability of their critical resources and restore the service to normality. In healthcare, unavailability of critical resources can have serious impact on patient health. During the WannaCry

attack, the affected NHS hospital had to cancel lifesaving operations and in some cases divert ambulances to far away hospitals that were not affected by the ransomware [39].

- Mean Time To Failure (MTTF). This metric could be used to measure the resilience of the systems in terms of the frequency and length of time between failures [78]. Reliability of systems is critical to most organisation but it is more so in the healthcare sector given the number of legacy systems in use and impact it will have on service delivery.
- Availability of offline and tested backups. This metric could be used to measure the reliability of the backups. Sometime backup might be the only option to restore services in some cases such as ransomware attacks. Organisation with a tested offline backup are less likely to end up with encrypted backup given malware developer are known to target online back to force victims to meet their demands [79].

H. Intelligence Driven Defence Metric

Cyberthreat intelligence is gaining popularity due to its proactive approach. Security professionals are using threat intelligence to learn more about intruders who are targeting their industry [80]. Threat intelligence usually depends on the existence of a vulnerability and the availability of a threat that could exploits the weakness [81]. There are several threat intelligence models that are widely used in the industry including the Cyber-kill chain, Diamond model, OWASP and Attack graphs [82]. The cyber-kill chain is intelligence driven defence approach that could be used to prevent attacks by disrupting the attackers activities at any of the seven stages described in the model [83]. The Diamond model allows security professionals to understand the behaviour and capabilities of the intruder and has four features which are: Infrastructure, capability, adversary and victim [84]. The Cyber-kill chain could be used to quickly determine the severity of attacks by mapping events produced by the various sensors. For example events from a Host Intrusion Prevention Systems(HIPS) could mean the attacker has gone past the early stage of the attack process and is on the installation or exploitation stage, therefore a high priority will need to be assigned to deal with such attack [85]. Examples of threat intelligence metrics that could be used to enhance protection are:

- Threat intelligence teams. This metric could be used to measure the technical resource capability. In-house threat intelligence teams can go through the internal and external threat intelligence databases and remove any false positives [86].
- Number of known threats groups targeting your organisation or sector at any given time. This metric could be used to measure how well you are capable of dealing with threats from these communities. Historical data could be used to analyse their pattern of behaviour. The data relating to these groups could be obtained from in-house intelligence teams or from vendors and security community at large.
- Number of attacks detected and mitigated using the attack models such as the Cyberkill chain. This could be an indication of how well your threat intelligence teams are performing. Information from such metric could be used to also protect your organisation from future attacks as part of lesson learnt.
- Access to vendor threat intelligence report directly related to your organisation. Vendors have huge capabilities and resources including threats sharing with their industry partners. Having access to these threats intelligence feeds will provide your organisation with an edge over the attackers.
- Metric from Indicators of Compromise(IOC). These metric was discussed in the sub-section above.
- Knowledge of online forums where exploits are sold or discussed. This metric will not only show how active your security teams are, but it is also one of the best ways to find how the threat actors are sharing newer techniques to exploit vulnerabilities.

I. Summary

In the security metrics section we categorised the metrics into eight different categories that could be used to calculate the security of the systems and to help decision-makers to make informed judgements. We discussed the challenges facing the healthcare sector and believe these metrics could help mitigate some of these cyber risks by strengthening the security defence mechanisms and instilling proactive security culture in these institutions.

Although these metrics could be used in any organisation, they are also well suited to healthcare environments where the complexity of the endpoints is high and the attack surface is larger due to presence of legacy systems and interconnected medical devices. These metrics will give visibility of the overall security once quantified and will also allow system administrators to react more quick to close loopholes. Metrics such as those for Red teaming could also be used during the optimisation stages after new security programs are deployed by testing the security defences of these systems.

IV. Conclusion

In this paper we discussed the security challenges facing the healthcare sector and provided some of the reason why this sector is susceptible to cyber attacks. Cyberattack is an issue affecting all industries and it is not just unique to the healthcare but the impact is far greater given it involves patient safety. The vulnerabilities of medical devices, infrastructure and security culture were discussed. Finally a cybersecurity metrics for enhancing the protection of these systems was proposed. The metrics were grouped into IOC, IOA, Penetration testing , Red and Blue teaming, Risk assessment, Resilience and Intelligence driven defence. Future work will involve quantifying and aggregating these metrics to provide a higher level view of

the security status of the networked systems including medical devices and other connected system.

REFERENCES

[1] C. Smith, "Cybersecurity implications in an interconnected healthcare system," *Frontiers of health services management*, vol. 35, no. 1, pp. 37–40, 2018.

[2] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[3] R. Koppel, S. W. Smith, J. Blythe, and V. Kothari, "Workarounds to computer access in healthcare organizations: you want my password or a dead patient?" *Booktitle=ITCH*, pp. 215–220, 2015.

[4] R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, "Risk-driven security metrics development for an e-health iot application," in *2015 Information Security for South Africa (ISSA)*. IEEE, 2015, pp. 1–6.

[5] Verizon, "Verizon data breach investigations report," Verizon, Report, 2018.

[6] SecurityScorecard, "The securityscorecard healthcare report," SecurityScorecard, Report, 2018.

[7] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *Journal of medical Internet research*, vol. 20, no. 5, 2018.

[8] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[9] E. D. Perakslis, "Cybersecurity in health care," *N Engl J Med*, vol. 371, no. 5, 2014.

[10] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?" *Bmj*, vol. 358, p. j3179, 2017.

[11] R. Priya, S. Sivasankaran, P. Ravisasthiri, and S. Sivachandiran, "A survey on security attacks in electronic healthcare systems," in *Communication and Signal Processing (ICCSP), 2017 International Conference on*. IEEE, 2017, pp. 0691–0694.

[12] S. Biddle. (2017, November) Securing wi-fi access for healthcare. [Online]. Available: https://www.fortinet.com/blog/industry-trends/securing-wi-fi-access-for-healthcare.html

[13] M. Mago and F. F. Madyira, "Ransomware software: Case of wannacry," *Engineering and Science*, vol. 3, no. 1, pp. 258–261, 2018.

[14] S. Mansfield-Devine, "Ransomware: taking businesses hostage," *Network Security*, vol. 2016, no. 10, pp. 8–17, 2016.

[15] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware a case study of wannacry ransomware," *arXiv preprint arXiv:1709.08753*, 2017.

[16] (2019, January) Ransomware corrupts 24,000 patient records of california specialist. [Online]. Available: https://healthitsecurity.com/news/ransomware-corrupts-24000-patient-records-of-california-specialist

[17] T. Yang, Y. Yang, K. Qian, D. C.-T. Lo, Y. Qian, and L. Tao, "Automated detection and analysis for android ransomware," in *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*. IEEE, 2015, pp. 1338–1343.

[18] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5–9, 2016.

[19] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Computers & Security*, vol. 74, pp. 144–166, 2018.

[20] N. Scaife, P. Traynor, and K. Butler, "Making sense of the ransomware mess (and planning a sensible path forward)," *IEEE Potentials*, vol. 36, no. 6, pp. 28–31, 2017.

[21] P. Padmanabhan. (2017, May) The nhs ransomware event and security challenges for the u.s healthcare system. [Online]. Available: https://www.cio.com/article/3196706/cyber-attacks-espionage/the-nhs-ransomware-event-and-security-challenges-for-the-u-s-healthcare-system.html

[22] J. Davies. (2018, 2018-12-19) The 10 biggest u.s. healthcare data breaches of 2018. [Online]. Available: https://healthitsecurity.com/news/the-10-biggest-u.s.-healthcare-data-breaches-of-2018

[23] C. Dennis, "Why is patch management necessary?" *Network Security*, vol. 2018, no. 7, pp. 9–13, 2018.

[24] D. W. Bates, A. Heitmueller, M. Kakad, and S. Saria, "Why policymakers should care about ?big data? in healthcare," *Health Policy and Technology*, 2018.

[25] M. Bamiah, S. Brohi, S. Chuprat *et al.*, "A study on significance of adopting cloud computing paradigm in healthcare sector," in *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on*. IEEE, 2012, pp. 65–68.

[26] A. Iyengar, A. Kundu, and G. Pallis, "Healthcare informatics and privacy," *IEEE Internet Computing*, vol. 22, no. 2, pp. 29–31, 2018.

[27] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *Ieee Access*, vol. 6, pp. 464–478, 2018.

[28] W. Liu, E. Park, S. Zhu, and U. Krieger, "An edge device centric e-health interconnection architecture," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018, pp. 1–5.

[29] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices (Auckland, NZ)*, vol. 8, p. 305, 2015.

[30] S. Schwartz, A. Ross, S. Carmody, P. Chase, S. C. Coley, J. Connolly, C. Petrozzino, and M. Zuk, "The evolving state of medical device cybersecurity," *Biomedical instrumentation & technology*, vol. 52, no. 2, pp. 103–111, 2018.

[31] Deloitte, "Cybersecurity of network- connected medical devices in the netherlands 2015," Deloitte, Report, 2015.

[32] U. Food, D. Administration *et al.*, "Postmarket management of cybersecurity in medical devices," 2016.

[33] ——, "Fda safety communication: cybersecurity for medical devices and hospital networks," *Retrieved May*, vol. 1, p. 2014, 2013.

[34] S. Anderson and T. Williams, "Cybersecurity and medical devices: Are the iso/iec 80001-2-2 technical controls up to the challenge?" *Computer Standards & Interfaces*, vol. 56, pp. 134–143, 2018.

[35] J. Sametinger, J. W. Rozenblit, R. L. Lysecky, and P. Ott, "Security challenges for medical devices." *Commun. ACM*, vol. 58, no. 4, pp. 74–82, 2015.

[36] A. Yadav, S. Raisurana, and P. Lalitha, "Information security in healthcare organizations using low-interaction honeypot intrusion detection system," *INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS*, vol. 11, no. 9, pp. 95–107, 2017.

[37] K. Wellington, "Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions," *Santa Clara High Tech. LJ*, vol. 30, p. 139, 2013.

[38] H. Thimbleby, *Addressing Systems Safety Challenges, Proc. 22nd Safety-Critical Systems Symp*, ser. Safety versus security in healthcare IT. CreateSpace Independent Publishing Platform, 2014.

[39] Cisomag. (2018, September) Nhs digital appoints first chief information security officer. [Online]. Available: https://www.cisomag.com/nhs-digital-hires-its-first-chief-information-security-officer/

[40] (2017, October) Nhs workers warned about consequences of snooping into patients' medical records. [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/nhs-workers-warned-about-consequences-of-snooping-into-patients-medical-records/

[41] F. Caldicott, "National data guardian for health and care," *Review of data security, consent and opt-outs*, 2016.

[42] S. Brannan, R. Campbell, M. Davies, V. English, R. Mussell, and J. C. Sheather, "Report from the national data guardian for health and care," 2016.

[43] K. P. Joshi, Y. Yesha, T. Finin *et al.*, "An ontology for a hipaa compliant cloud service," in *4th International IBM Cloud Academy Conference ICACON 2016*, 2016.

[44] Thycotic, "State of cybersecurity metrics annual report," Thycotic, Report, 2017.

[45] G. Campbell, *Measures and metrics in corporate security*. Elsevier, 2014.

[46] W. Jansen, *Directions in security metrics research*. Diane Publishing, 2010.

[47] C. W Krag Brotby and G. Hinson, *Pragmatic security metrics: applying metametrics to information security*. Auerbach Publications, 2016.

[48] E. Chew, M. M. Swanson, K. M. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance measurement guide for information security," Tech. Rep., 2008.

[49] R. M. Savola, "Towards a taxonomy for information security metrics," in *Proceedings of the 2007 ACM workshop on Quality of protection*. ACM, 2007, pp. 28–30.

[50] L. Hayden, *IT security metrics: A practical framework for measuring security & protecting data*. McGraw-Hill Education Group, 2010.

[51] K. N. Mallikarjunan, S. M. Shalinie, K. Sundarakantham, and M. Aarthi, "Evaluation of security metrics for system security analysis," in *Computational Intelligence: Theories, Applications and Future Directions-Volume I*. Springer, 2019, pp. 187–197.

[52] Y. Ahmed, S. Naqvi, and M. Josephs, "Aggregation of security metrics for decision making: a reference architecture," in *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*. ACM, 2018, p. 53.

[53] S. Jafari, F. Mtenzi, R. Fitzpatrick, and B. O?Shea, "Security metrics for e-healthcare information systems: a domain specific metrics approach," *Int. Journal of Digital Society*, vol. 1, no. 4, pp. 238–245, 2010.

[54] V. Liu, A. D. Tesfamicael, W. Caelli, and T. Sahama, "Network security metrics and performance for healthcare systems management," in *E-health Networking, Application & Services (HealthCom), 2015 17th International Conference on*. IEEE, 2015, pp. 189–194.

[55] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and ?, 2012, pp. 269–275.

[56] S. M. Muthukrishnan and S. Palaniappan, "Security metrics maturity model for operational security," in *Computer Applications & Industrial Electronics (ISCAIE), 2016 IEEE Symposium on*. IEEE, 2016, pp. 101–106.

[57] T. Micro. (2018) Indicators of compromise. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise

[58] P. I. LLC, "2018 cost of a data breach study: Global overview," Report, July 2018.

[59] S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*. ACM, 2015, pp. 43–49.

[60] (2017, May) Indicators associated with wannacry ransomware. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-132A

[61] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, vol. 72, pp. 212–233, 2018.

[62] (2018, June). [Online]. Available: https://www.fireeye.com/services/freeware/redline.html

[63] (2019, March) Ioc-bucket. [Online]. Available: https://iocbucket.com

[64] (2019) Ioc editor. [Online]. Available: https://www.fireeye.com/services/freeware/ioc-editor.html

[65] O. Catakoglu, M. Balduzzi, and D. Balzarotti, "Automatic extraction of indicators of compromise for web applications," in *Proceedings of the 25th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2016, pp. 333–343.

[66] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *Journal of Network and Computer Applications*, vol. 101, pp. 18–54, 2018.

[67] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu, "Torward: Discovery, blocking, and traceback of malicious traffic over tor," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2515–2530, 2015.

[68] N. Veerasamy, "Cyber threat intelligence exchange: A growing requirement," 2017.

[69] E. Purvine, J. R. Johnson, and C. Lo, "A graph-based impact metric for mitigating lateral movement cyber attacks," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*. ACM, 2016, pp. 45–52.

[70] B. K. Devi, G. Preetha, and S. M. Shalinie, "Ddos detection using host-network based metrics and mitigation in experimental testbed," in *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on*. IEEE, 2012, pp. 423–427.

[71] J. Hoffmann, "Simulated penetration testing: From" dijkstra" to" turing test++"." in *ICAPS*, 2015, pp. 364–372.

[72] (2019, March) Attackiq intelligent security decissions. [Online]. Available: https://www.attackiq.com

[73] J. N. Goel and B. Mehtre, "Vulnerability assessment & penetration testing as a cyber defence technology," *Procedia Computer Science*, vol. 57, pp. 710–715, 2015.

[74] S. Mansfield-Devine, "The best form of defence–the benefits of red teaming," *Computer Fraud & Security*, vol. 2018, no. 10, pp. 8–12, 2018.

[75] A. Applebaum, D. Miller, B. Strom, C. Korban, and R. Wolf, "Intelligent, automated red team emulation," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*. ACM, 2016, pp. 363–373.

[76] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, 2016.

[77] W. Harrop and A. Matteson, "Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the uk and usa," in *Current and Emerging Trends in Cyber Operations*. Springer, 2015, pp. 149–166.

[78] W. Torell and V. Avelar, "Mean time between failure: Explanation and standards," *white paper*, vol. 78, 2004.

[79] H. Orman, "Evil offspring-ransomware and crypto technology," *IEEE Internet Computing*, vol. 20, no. 5, pp. 89–94, 2016.

[80] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. ACM, 2014, pp. 51–60.

[81] Webroot, "Threat intelligence: What is it,and how can it protect you from today's advanced cyber-attacks?" Webroot, Tech. Rep., 2014.

[82] H. Al-Mohannadi, Q. K. Mirza, A. Namanya, I. U. Awan, A. J. Cullen, and J. F. Pagna Disso, "Cyber-attack modeling analysis techniques: An overview," 2016.

[83] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 438–452.

[84] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *Intelligence and Security Informatics Conference (EISIC), 2017 European*. IEEE, 2017, pp. 91–98.

[85] L. M. Corporation, 2015.

[86] D. Shackleford, "Who's using cyberthreat intelligence and how?" *SANS Institute. Retrieved January*, vol. 24, p. 2018, 2015.