5G CYBERSECURITY: RISK ASSESSMENT AND INCIDENT RESPONSE IN THE HEALTHCARE INDUSTRY

Yit Loong Teh[1*], Yao Tong Tan[1], and Siaw Lang Wong[1]

[1] Faculty of Computing and Information Technology, Tunku Abdul Rahman University College, Kampus Utama, Jalan Genting Kelang, 53300, Wilayah Persekutuan Kuala Lumpur, Malaysia
*Corresponding author: tehelon@gmail.com

ABSTRACT

Rapid proliferation and developments in the field of telecommunication have led to a renewed interest in the fifth-generation technology standard for broadband cellular networks. As compared to the previous generations, 5G is capable of connecting numerous nodes simultaneously while offering pathbreaking implementations in enabling time-critical services such as autonomous vehicles, real-time drone manoeuvres, Industry 4.0, virtual reality, augmented reality, etc. Nevertheless, these conveniences may turn out to be security threats or vulnerabilities susceptible to cyberattacks. Apparently, thwarting cyberattacks is a never-ending journey, especially in the major economic sector – healthcare. It is an undeniable fact that healthcare is among the industries underpinning a nation's economy. Hence, this paper will first forecast the trend of PHI breaches with Holt Winter's model to emphasise the rise of cyber threats. Next, evaluating the risks of the chosen asset with ISO/IEC 27001 risk matrix. Then, compares the National Institute of Standards and Technology (NIST) SP 800-61 Incident Response Lifecycle and John Boyd's OODA Loop; the latter offers significant advantages over the former concerning the adoption of situational awareness concepts, philosophy, and more. As a result, the number of PHI breaches increase tremendously due to the growth in the number of IT incidents and insider attacks.

Keywords: 5G network, Incident response, Agile response, Cyberattack, Information security

List of notations

L_t is the value of Level
T_t is the value of Trend
S_t is the value of Seasonality
Y_t is the last period value

1.0 INTRODUCTION

From the top, a mobile network, or otherwise known as the cellular network is a type of wireless network utilising radio waves to transmit data (Ramachandran *et al.*, 2021). To date, there are five generations of cellular networks, with each providing different capabilities. Nonetheless, the fifth-generation cellular network is a game-changer as it offers lots of new features and opportunities like never before. Such technology otherwise known as 5G, introduces a ground-breaking kind of network that is neither confined by the context of only improved access to the internet services, nor only better phone call quality. But it is capable of connecting everyone and everything as today's world is packed with the Internet of Things (IoT) devices (Liyanage *et al.*, 2018). 5G unleashes its potentials by promoting earth-shattering benefits such as delivering sky-high peak data speeds, massive bandwidth,

extremely low latency, supporting millions of IoT devices, enabling smart cities, and so on (Bendale and Rajesh Prasad, 2018).

However, it is tremendously difficult to achieve a perfect balance between rapid technological advancement and the risks they pose to the users. Hence, these advantages offered by 5G may turn into security risks that will threaten all involved aspects and elements. Additionally, the preponderant influence of 5G has left its security concerns and risks behind. This causes numerous governments and industries to be in a hurry to set up and deploying 5G-related technologies just to keep themselves up to par with the new national broadband standard without considering its security concerns thoughtfully (Arias *et al.*, 2020). Significantly, 5G itself may be susceptible to various cyberattacks and may indirectly facilitate other cyberattacks to be carried out. Since cybersecurity is a never-ending journey, users have to always be prepared to brace for impacts. For the time being, there are only a meagre number of cybersecurity incident handling strategies designed for 5G-related incidents.

Thus, this paper addresses the issues by evaluating two incident response (IR) models to determine if they are still feasible in containing evolved cyberattacks facilitated by 5G, including the NIST SP 800-61 Incident Response Lifecycle and John Boyd's OODA Loop. Particularly, the assessment and discussion will be encompassing the context of two industries: healthcare and online retail since they are the potential heavy users of the 5G network (Gohar and Nencioni, 2021). These industries are also playing important roles in pushing smart cities forward. Nonetheless, such that there is a cyberattack capable of bringing down the entire smart city including the power grid, internet connection, and more, cutting-edge IoTs such as autonomous drones will no longer work. Therefore, an agile incident management plan must be there ensuring the continuity of service.

An agile cybersecurity incident handling strategy is different from the traditional ones. The latter will usually be a static framework that is designed to contain pre-emergent cyberattacks. They are designed without the consideration of a network that is dealing with an array of new technologies such as network slicing, fog and cloud computing, IoT, etc. On the other hand, the former considers surrounding data gathered before a decision is made. An agile model is also known as a 'data-driven model' that gives the IR team some insights into the causes of the incident (Sun *et al.*, 2019). For instance, the team may come up with a hypothesis where the alerts generated by an Intrusion Detection System (IDS) indicating there is an incident happening on the network.

The rest of the paper is organised as follows. In Section 2, the background study and related work in 5G security are reported. Next, the methodology of the study is discussed in Section 3. Section 4 presents the results and discussions. Section 5 concludes the paper.

2.0 BACKGROUND AND RELATED WORKS

This section consists of four sub-sections. Sub-section 2.1 wrapped up the potential applications of the 5G and its associated technologies in the healthcare industry. Then, sub-sections 2.2 and 2.3 emphasised the increased PHI breaches over the past ten years due to hacking, IT incidents, and unauthorised disclosure and introduced several cyberattacks that may pose security threats to the facilities, respectively. Sub-section 2.4 indicated that the current IR strategies need improvements to cope with the 5G environment.

2.1 5G and Its Application in the Healthcare Industry

In light of the 5G network's deployment, industries began to transform or upgrade their business operations, especially the healthcare industry. With reference to Li (2019), the potential applications are remote diagnosis, autonomous ambulance, smart hospital, Augmented Reality (AR) and Virtual Reality (VR) training, telemedicine, etc. Logically,

when the use of technologies has been widened, it expands the attack surface. Furthermore, one of the benefits of the 5G network offers is the enormous bandwidth. Gurusamy *et al.* (2019) have indicated that the Massive IoT (MIoT) concept will increase the size of an ordinary botnet tremendously. Thus, it pushes further the immediate need for a superlative IR strategy and response plan tailored for the healthcare industry. Medical practitioners are leveraging decent technologies associated with 5G like AR and VR to draw on the outcomes from their medical researches and also provisioning pre-operation simulation to get them prepared for the actual operation.

2.2 Cyber Threats Posed to the Healthcare Industry

Protected Health Information (PHI) is an alluring target for cybercriminals as this information can be used in various ways to make a profit illegally (Kasperbauer, 2020). Not to mention that more information can be extracted with the aid of big data analysis. Moreover, Bai *et al.* (2017) have found out that 53% of 1150 PHI leakages reported are caused by internal attacks, either advertently or unwittingly. The remaining 47% comprise of external attacks like hackers and other cybercriminals. Therefore, it is an undeniable fact that the roll out of 5G and its associated technologies may worsen the situation, especially when the cybercriminals started to utilise such technology to facilitate cyberattacks. Referring to HIPAA Journal (2020), the major causes of PHI breaches are hacking, Information Technology (IT) incidents, and unauthorised disclosures, refer to Figure 1. Unsurprisingly, the number of PHI breaches shot up apace with the emergence of technologies.

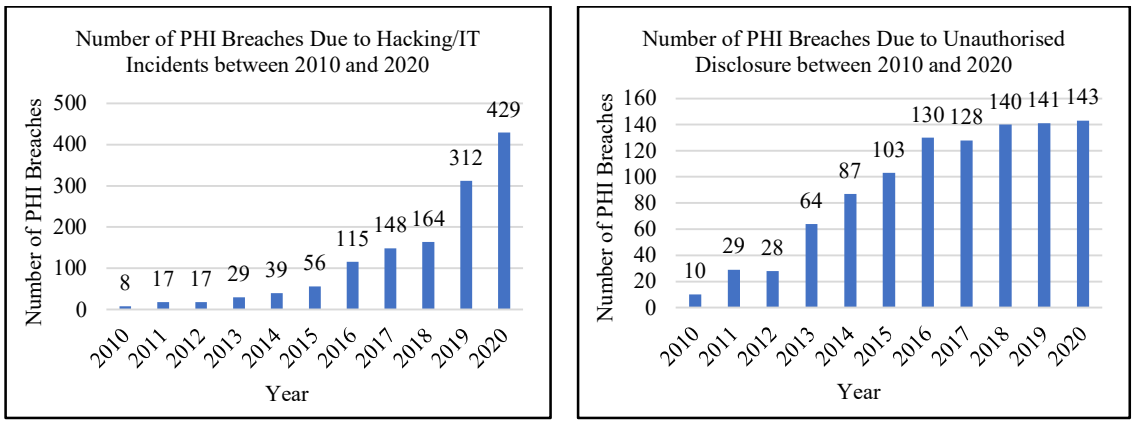


Figure 1. Number of reported data breaches in the healthcare industry due to (a) hacking/IT incidents and (b) unauthorised disclosure. Image source: HIPAA Journal (2020)

2.3 5G Cybersecurity Concerns

Because none of the technologies was made perfect, Hussain *et al.* (2019) have pointed out that the 5G radio network is susceptible to Tracking via Paging Message Distribution (ToRPEDO) attack. This attack allows a cybercriminal to inject fabricated paging messages and launch a Denial-of-Service (DoS) attack by spamming unnecessary paging messages. Not only that, Oliver (2021) has mentioned that most of the existing security vulnerabilities that exist in 3G and 4G will remain in 5G such as locating users, intercepting SMSs, initiating DoS attacks, etc.

2.4 5G Incident Management

According to Barona López *et al.* (2017), the existing IR strategies are not specifically designed for incidents in the context of the 5G network. This is due to the architectural design

of the 5G its associated technologies were not considered. The 5G network connects the infrastructure, hardware, software, data, people, and other components as a whole. However, these ordinary general-purpose models can be tailored to fit various organisational needs so long that the core structure of the response architecture is not affected.

3.0 METHODOLOGY

In this paper, Holt Winter's model was being used to forecast the trend of PHI breach incidents in the next five years, refer to equations (1) - (3). This model is feasible since such incidents happen periodically. The weekly seasonality was set to yearly seasonality, $m = 365$. Missing points were filled with interpolation method while duplicates were aggregated with the average value. Secondary data was gathered from HIPAA Journal that is available for public access online.

$$L_t = \alpha(Y_t - S_t - m) + (1 - \alpha)[L_t - 1 + T_t - 1] \quad (1)$$

$$T_t + 1 = \beta(L_t + 1 - L_t) + (1 - \beta)T_t \quad (2)$$

$$S_t = \gamma(Y_t - L_t) + (1 - \gamma)S_t - m \quad (3)$$

Next, a comparative, one asset will be chosen from the healthcare industry and to be assessed with the ISO/IEC 27001 risk matrix. In Table 1, the degree of impact is *significant* when the cyberattack threatens an asset's confidentiality disclosure, *serious* when there is an integrity breach, and *mild* when it challenges its availability.

Then, a comparative analysis was conducted between an ordinary cybersecurity IR model and a dynamic IR model with several metrics/criteria: number of steps, philosophy, situational awareness, hypothesis making, etc. In this context, the former is referring to the NIST SP 800-61 while the latter is the OODA Loop. These criteria were chosen because they are playing an influential role in facilitating the IR team to make a precise decision for containing an incident.

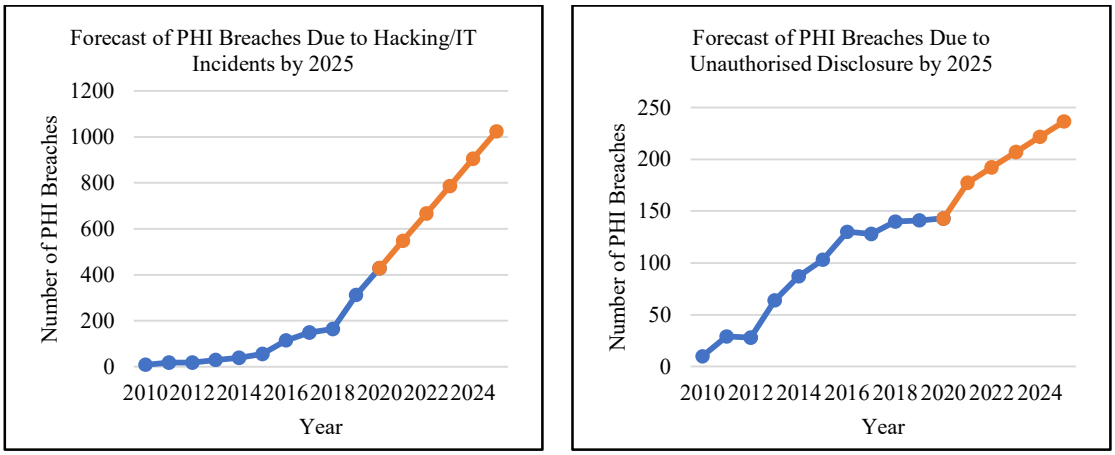
Table 1. ISO/IEC 27001 risk matrix.

	Threat Likelihood		
Degree of Impact	Low	Moderate	High
Significant (High)	2	3	3
Serious (Moderate)	1	2	3
Mild (Low)	1	1	2

4.0 RESULTS AND DISCUSSIONS

4.1 Forecast of PHI Breach Trend

With reference to Figure 2, the solid line in orange is referring to the predicted values. The trend of PHI breaches was predicted to increase 138.69% and 65.03% by 2025, respectively. In general, both types of PHI breaches are showing steep and almost consistent increments each year. At this point, there is a high likelihood of severe PHI breaches to happen in the coming years and it is also indicating that the commercialisation of the 5G and its associated technologies can also be one of the main factors that drive the figures up. As mentioned in the introduction, the 5G is still a new technology embeds with hidden vulnerabilities. Therefore, these forecasts have signified the need for a dynamic IR strategy.



(a) **(b)**

Figure 2. Forecast of reported data breaches in the healthcare industry due to (a) hacking/IT incidents and (b) unauthorised disclosure by 2025.

4.2 Cyber Risk Evaluation on PHI

With reference to Figure 3, PHI was adopted as the most anticipated asset for security protection by the healthcare industry players (Pool *et al.*, 2019). According to the researchers, PHI is the most difficult asset to protect against cyberattacks as it involves multiple parties in the use of these data such as medical practitioners, registrars, etc. Furthermore, this data is valuable to hackers as they are able to make ends meet by disclosing it to the public, trade it to a third party through the dark web, or just simply make it inaccessible for a certain reason. Also, they may illegally modify the data. From the findings, both threats are equally posing a very critical cyber risk to PHI, especially when it comes to confidentiality and integrity breaches. On top of that, Figure 2 have shown that the plausibility for a cybercriminal to target PHI is very promising. As a result, hackers and careless personnel are probable to impact PHI. Healthcare businesses should be prepared to brace for cyber impacts in future.

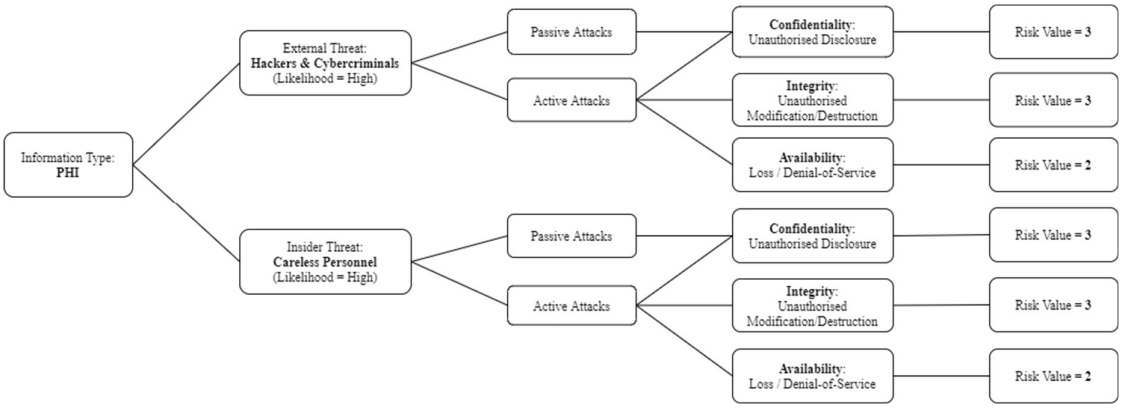


Figure 3. Evaluating cyber risk posed on PHI.

4.3 Comparison of IR Models

In the previous discussions, the need for a new IR model is a must when healthcare businesses started to adopt and deploy 5G technologies in their organisations. As mentioned and discussed in the literature review, the 5G networks connect including but not limited to people, data, infrastructure, hardware, and software. And the incident can happen on any one

of these elements. Hence, the new IR strategy must show a high degree of agility than ever before.

John Boyd's OODA Loop is a dynamic IR model which is different from the ordinary procedural NIST SP 800-61 Incident Response Lifecycle. The summary of differences as discussed in the literature review and the comparison are tabulated in Table 2.

Table 2. Summary of comparison between IR models.

	NIST SP 800-61	Boyd's OODA Loop
Number of Phases	4	4
Philosophy	Procedural and evidence-based	Data-driven
Situational Awareness	No	Yes
Unfolding Circumstances	No	Yes
Hypothesis Making	No	Yes

It is an undeniable fact where the world today is full of IoTs and surrounded by 5G-associated technologies such as smart cities, smart homes, smart factories, and more. In the healthcare context, As technology advances from day to day, the same goes for the evolvement of cyberattacks. Plus, the literature reviews have also raised some of the issues of the 5G network. At this point, the need for a dynamic IR model has been pushed further. Both IR models have four phases. One point that is noteworthy to mention is that the criteria of proceeding to the next phase are different and it varies from case to case. The philosophy of the NIST SP 800-61 Incident Response Lifecycle in identifying an incident is based on solid evidence provided. To further detail this, a good example would be an information espionage case where a suspicious individual extracted PHI data from a medical workstation and escaped from the building. From here, the evidence will be the workstation's system logs and the surveillance system's recordings. The lifecycle emphasises the analysis of evidence while collection and this will eventually cost more time to get to the eradication phase. In contrast, John Boyd's OODA Loop will be based on data gathered from the environment before a hypothesis is made. For example, the hypothesis can be the leakage of a patient's health information alongside other registered credentials. The formulation of the hypothesis will usually make use of experience and training knowledge. External key factors including culture and previous experience are to be taken into consideration.

Besides that, both internal and external key factors are accountable for the formulation of a hypothesis of what activities are involved in an incident. Correlation of anomaly activities can be done in the Orient phase or analysis phase of the NIST SP 800-61 Incident Response Lifecycle. Whenever any ambiguities are found in the phases, the team shall loop back to the Observation phase.

Not to mention that situational awareness helps the IR team to learn the attacker's activities, attribution, capabilities, and intelligence (Van Os, 2021). Another factor is the flexibility of IR models. John Boyd's OODA Loop has both Observe and Orient phases to gather and synthesis data and information from the incident environment. Such that the environment consists of millions of IoT devices including autonomous drones, cars, manufacturing facilities, smartwatches, smartphones, smart grids, and other relevant technologies, John Boyd's OODA Loop is certainly playing an influential role in halting a cyberattack. The NIST SP 800-61 Incident Response Lifecycle emphasises the procedural steps taken to ensure the completeness of the handling process while John Boyd's OODA Loop aims to minimise the impacts as quickly as possible.

Furthermore, the Plan-Do-Check-Act (PDCA) methodology used to formulate various business continuity strategies that have been included in ISO 22301 standard is a Boyd's OODA Loop lookalike. Nonetheless, Boyd's OODA Loop depends heavily on unfolding circumstances whereas both PDCA and NIST SP800-61 Incident Response Lifecycle do not. Boyd's OODA Loop has another unique characteristic called 'Survive with own terms'. Such a characteristic enables the model to focus on synthesising an action out of an incomplete data set since it is almost impossible to identify every variable in the environment that the IR team is forced to deal with (Sharp, 2020). Therefore, that contributes to the reason of making a hypothesis in which the IR team believes that a particular decision will result in the highest probability for success while reducing any potential security risks. The gist here is the formulation of action from the Observe and the Orient phases given that the IR team is placed in a complex and mysterious environment which subject to regular and unpredictable change. From here, it is related to the 5G and its associated technologies as the environment are still embedded with leashed potentials or even a potential superb cyber threat.

Since the NIST SP 800-61 is offering a procedural guideline in outlining cybersecurity frameworks, it primarily deduces the course of actions through thorough data analysis and step-to-step best practices. However, such a methodology will find it difficult to act proactively as it is a set of pre-planned procedures waiting to be executed. The 5G environment is consistently changing and truth to be told that fluidly changing plans and responses must be emphasised by businesses involved in the fourth industrial revolution like healthcare organisations.

5.0 CONCLUSIONS

All in all, this paper has discussed the future of PHI breaches alongside the implementation of the 5G and its associated technologies in the healthcare industry. This paper has foreseen that more and more PHI will be leaked due to the growth of IT incidents and unauthorised disclosure. With the aid of Holt Winter's seasonal model, healthcare businesses should be equipped with appropriate cyber defence strategies. In addition, this paper used ISO/IEC 27001 risk matrix to assess the level of risk posed to the PHI since it is playing an influential role in bridging medical practitioners and their patients. As a result, it shows that PHI is at risk in face of the worsening situation. Hence, the gradual need for a dynamic IR model alongside the emergence of 5G-associated technologies has been signified through the findings. Moreover, the comparison between IR models in terms of their philosophies, implementation of situational awareness concept, etc. have shown that John Boyd's OODA Loop is the potential IR model that offers significant advantages over the NIST's SP 800-61 Incident Response Lifecycle given that it has a higher degree of dynamicity in inferring actions to be taken in the face of cybersecurity incidents.

6.0 ACKNOWLEDGMENTS

The authors would like to thank the Faculty of Computing and Information Technology, Tunku Abdul Rahman University College for the financial support and resources to carry out this study. Besides that, the authors would also like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

Arias, R. et al., 2020. *The Impact of 5G: Creating New Value across Industries and Society*, The World Economic Forum.

Bai, G., Jiang, J. (Xuefeng) and Flasher, R., 2017. Hospital Risk of Data Breaches. *JAMA Internal Medicine*, 177(6), p.878. Available at: http://annals.org/article.aspx?doi=10.7326/M15-2886.

Barona López, L. et al., 2017. Towards Incidence Management in 5G Based on Situational Awareness. *Future Internet*, 9(1), p.3. Available at: http://www.mdpi.com/1999-5903/9/1/3.

Bendale, S.P. and Rajesh Prasad, J., 2018. Security Threats and Challenges in Future Mobile Wireless Networks. *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. November 2018 IEEE, pp. 146–150.

Gohar, A. and Nencioni, G., 2021. The role of 5g technologies in a smart city: The case for intelligent transportation system. *Sustainability (Switzerland)*, 13(9), pp.1–24.

Gurusamy, D., Deva Priya, M., Yibgeta, B. and Bekalu, A., 2019. DDoS risk in 5G enabled iot and solutions. *International Journal of Engineering and Advanced Technology*, 8(5), pp.1574–1578.

HIPAA Journal, 2020, *Healthcare Data Breach Statistics* [Online]. Available at: https://www.hipaajournal.com/healthcare-data-breach-statistics/ [Accessed: 10 October 2021].

Hussain, S.R. et al., 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. *Proceedings 2019 Network and Distributed System Security Symposium*. 2019 Internet Society, Reston, VA.

Kasperbauer, T.J., 2020. Protecting health privacy even when privacy is lost. *Journal of Medical Ethics*, 46(11), pp.768–772. Available at: https://jme.bmj.com/lookup/doi/10.1136/medethics-2019-105880.

Li, D., 2019. 5G and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare? *Precision Clinical Medicine*, 2(4), pp.205–208.

Liyanage, M. et al., 2018. 5G Privacy: Scenarios and Solutions. *2018 IEEE 5G World Forum (5GWF)*. July 2018 IEEE, pp. 197–203.

Oliver, D., 2021, *5G security: everything you need to know about the security of 5G networks* [Online]. Available at: https://www.5gradar.com/features/5g-security-5g-networks-contain-security-flaws-from-day-one [Accessed: 14 October 2021].

Van Os, R., 2021, *The added value of the OODA loop to cyber security - part 3/3* [Online]. Available at: https://www.linkedin.com/pulse/added-value-ooda-loop-cyber-security-part-33-rob-van-os?trk=public_profile_article_view [Accessed: 9 September 2021].

Pool, J.K., Akhlaghpour, S., Fatehi, F. and Burton-Jones, A., 2019. Causes and Impacts of personal health Information (PHI) Breaches: A scoping review and thematic analysis. *Proceedings of the 23rd Pacific Asia Conference on Information Systems: Secure ICT Platform for the 4th Industrial Revolution, PACIS 2019*, (April 2020).

Ramachandran, T., Faruque, M.R.I., Siddiky, A.M. and Islam, M.T., 2021. Reduction of 5G cellular network radiation in wireless mobile phone using an asymmetric square shaped passive metamaterial design. *Scientific Reports*, 11(1), p.2619. Available at: https://doi.org/10.1038/s41598-021-82105-7.

Sharp, D., 2020, *Planning ahead: The OODA vs PDCA methodology* [Online]. Available at: https://www.ideagen.com/thought-leadership/blog/planning-ahead-ooda-vs-pdca-methodology [Accessed: 12 October 2021].

Sun, N. et al., 2019. Data-Driven Cybersecurity Incident Prediction: A Survey. *IEEE Communications Surveys & Tutorials*, 21(2), pp.1744–1772. Available at: https://ieeexplore.ieee.org/document/8567980/.