Available online at
http://journal.uitm.edu.my/ojs/index.php/BEJ

e-ISSN: 2637-0395

Built Environment Journal 21(Special Issue) 2024, 49 – 58.

Built Environment Journal

Impacts of Cybersecurity Threats on Construction Stakeholders in Malaysia Amidst Industrial Revolution 4.0

Ramli Isa[1], Har Einur Azrin Baharuddin[1*], Airul Faizal Othman[2]

[1]Studies of Quantity Surveying, College of Built Environment, Universiti Teknologi MARA, 40450 Shah Alam, Selangor
[2]Public Works Department (PWD), Kuala Lumpur, 50350, Malaysia

ARTICLE INFO

Article history:
Received 1 June 2024
Revised 19 August 2024
Accepted 30 August 2024
Online first
Published 30 September 2024

Keywords:
Industrial Revolution 4.0 (IR 4.0)
Cybersecurity
Threats
Stakeholders
Construction

DOI:
10.24191/bej.v21iSpecial Issue.1598

ABSTRACT

Cybersecurity is one of the elements of IR 4.0 which is created to provide security and protect digital information which includes construction industry from expose to cybersecurity threat. Cyberthreats happen to any digital device and working in digitalisation environment, files will be shared online, everyone can access those files if it does not provide a security password to open it. There are ways to overcome and minimise cybersecurity threats which need to be explored to avoid threats. Thus, the aim is to explore the impacts of the cybersecurity threats among stakeholders in construction in IR 4.0. The objectives are to identify the potential threats of cybersecurity on construction stakeholders in Malaysia, followed by recommendation ways to improve the implementation of cybersecurity usage among stakeholders and minimise threats incidents for safety purposes for construction stakeholders' company. The data obtained using quantitative method where the random sampling survey conducted through distribution of questionnaire to stakeholders in construction. Findings show that, cybersecurity systems in construction are not very deep because currently the construction sector is not a major contributor in cyber security intrusions and threats. Stakeholders in construction implement cybersecurity measures such as use of anti-virus, regular software update etc., which most of these are related to their task where all work is now completed using digitalised gadget. In terms of ways to improve the implementation of cybersecurity usage among stakeholders and minimise threats incidents, it can be concluded that individual approach is the most effective way medium to overcome this problem.

[1*] Corresponding author. *E-mail address*: hareinur@uitm.edu.my
https://doi.org/10.24191/bej.v21iSpecial Issue.1598

INTRODUCTION

The growing interconnectivity and data exchange among devices and systems in Industry 4.0 present novel cybersecurity challenges that must be addressed to safeguard critical infrastructure, sensitive data, and intellectual property. Industrial Revolution 4.0 (IR 4.0) encourages the widespread use of Internet of Things (IoT) in various applications, which necessitates robust cybersecurity measures to protect the information shared across multiple devices. Cybersecurity is the method used to provide security to the network or protect the cyber from any threat to happen in cyber. According to Rossouw von Solms & Johan Van Niekerk (2013), cybersecurity as tools, regulations, security principles, guidelines, risk management techniques, activities, training, best practices, assurance, and technologies that can be employed to defend an organisation's and its users' interests in the cyberspace. Which mean cybersecurity is used to protect the assets of user and organisation which involve in the component that consist in digitalisation system such as device which computer, smartphone, smart application, telecommunication device and other related to digitalisation component. While cybersecurity threats are according to (Al Zaidy, 2014) cyber threat defines as cyberattacks encompass any form of attack or threat directed towards a computer where it is connected to the internet through a network. Thus, cyber threats can happen to any digital device that is connected to the internet network. Architects and contractors may suffer financial losses as a result of malicious hackers using vulnerabilities to alter payment approvals, divert funds, or commit fraud. Hence, cybersecurity is essential to preventing payment data manipulation. Without adequate security, payment information such as amounts, project deadlines, or recipient details may be changed, resulting in erroneous transactions and inaccurate project finance. Without a doubt, when clients and architects communicate during the building process without cybersecurity safeguards in place, both sides may be exposed to different risks associated with data breaches. Therefore, it is essential for stakeholders in construction—such as engineers, architects, quantity surveyors, and project personnel involved in (Information Technology) IT, who deal with cloud systems, or data management—to explore additional initiatives aimed at mitigating this growing issue. It is crucial to understand the impact of cybersecurity systems on construction stakeholders, including discussing the challenges and proposing a way forward to ensure secure practices in construction projects. Therefore, it is important to understand that are the potential threats and way to recommends in order to prevent the cybersecurity scrutinising the digitalisation of construction industry.

LITERATURE REVIEW

Definition of cybersecurity

Generally, cybersecurity is the method used to provide security to the network or protect the cyber from any threat to happen in cyber. According to Rossouw von Solms & Johan Van Niekerk, (2013), cybersecurity as tools, regulations, security principles, guidelines, risk management techniques, activities, training, best practices, assurance, and technologies that can be employed to defend an organisation's and its users' interests in the cyberspace. Which mean cybersecurity is used to protect the assets of user and organisation which involve in the component that consist in digitalisation system such as device which computer, smartphone, smart application, telecommunication device and other related to digitalisation component. This was supported by Seemma et al., (2018), cyberattacks are prevented by internet-connected devices, including data, software, and hardware. Which means that cybersecurity can be protected by the use of systems that are connected to the internet network. According to Mantha & De Soto (2019), cyber security is a policy, and tools obtained to provide protection against data that has been saved and sent which include contract documents, drawings and related schedule. The definition given is more specific for construction fields which involve drawings and important contracting have been made. So here it is easy to say that cybersecurity is constructed with an objective to provide security and protecting the digitalisation system from threat and hacking by others. As the living in digitalisation era and the demand is increasing all day which this cause of the requirement for cybersecurity as a crucial method to protecting the individuals and organisations from security breach or other online crimes such as malware, hacking, etc.

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

The awareness of cyber threats

Once inside the digitalisation system, a cyber threat is going to occur from hackers. According to (Al Zaidy, 2014) cyber threat defines cyberattacks encompassing any form of attack or threat directed towards a computer where it is connected to the internet through a network. So, cyber threats can happen to any digital device that is connected to the internet network. A hacker defines as a person who employs technical know-how to gain unauthorised access to data in order to change, remove, or sell it in any way (Maalem Lahcen et al., 2020). Hackers are often the ones who carry out cyber threats. Hackers with malevolent intent often take advantage of holes in computer systems or networks to launch cyberattacks. These assaults may be intended to spread malware, steal confidential data, interfere with services, or inflict other types of damage. Cyber threat and hacker are related to each other. As mentioned, it is a cyber which requires the internet network to access cyberspace services. While cyberattacks are acts carried out by nations to breach a nation's or another nation's computer systems in order to cause harm or disruption (Li & Liu, 2021). According to (De Bruijn & Janssen, 2017), cybersecurity threats can happen, and it is relying on internet access. To access cyberspace, internet access is required, and this causes the cyberthreat to happen as there is internet interaction happen. Through this cyberattack, it can cause a critical problem to the sensitive information of a country. Even though the country is a large region, when cyber threats occur, it still has a negative impact on the country. It is very dangerous for this cyber threat that should be curbed from causing worse effects in the future. It is even more dangerous when even the smallest sector of the industry is hacked to leak important information and make a threat to the industry. In short, where there is access to the cyber world, there will be cyber threats that will occur regardless of the size of the organisation, the danger will still arise.

National Construction Policy 2030

National Construction Policy 2030 (NCP 2030) aim to encourage the construction sector and all the stakeholder in the construction to prepare and show the readiness to involving themselves in the new technologies and keep up to date of the latest issues arise in the global stage. Furthermore, to make a transformation of the construction sector moving towards the digitalisation era. This was supported by the Ministry of Works which to support and stand for the Malaysian construction industry towards international recognition. The NCP 2030 shows that the construction industry in Malaysia is growing to upgrade the construction sector to the level of digitisation which means it is presenting the construction industry in Malaysia growing in line with the speed and advancement of the latest technology. Previous study conducted by Ranstad Work monitor in the second quarter of 2019 has shown that 89% of the employers still lack skills in digitalisation development. So, the suggestion to this problem is that some investment should be made to make sure that the employers are able to learn digital skills development so that it can grow the construction industry to the level which the optimum of digital skills. It is still not too late to invest in the construction sector as the demand for construction products is increasing all the time. In other words, it is worth learning and empowering the digital skills development. But the government proposed initiative which the digitalisation in the NCP is to make sure the construction industry benefited the people's prosperity. To encourage the stakeholders in construction towards digitalisation, the government tries to produce productivity of construction with the optimum used of technologies.

METHODOLOGY

The early stage of the research starts with a comprehensive desktop search conducted under the "title/abstract/keyword" field from several dominant multi-disciplinary databases in the year between 2019 and 2023. Then, from the publication databases, the initial search was done using the "cybersecurity", cyber threats, NCP 2030, stakeholder in construction". Numerous studies have investigated cybersecurity and its threats from different perspectives to look on the impact toward construction stakeholders. Then, this research adopts a quantitative approach through a random sampling technique in collecting data from the stakeholders namely Architects, Quantity Surveyors, Engineers, Contractors company, IT/Technical

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

department of the firm. The reason of using random sampling is because the capacity in creating smaller sample size for a larger population group (Kumar, 2019). The idea behind random sampling makes it suitable for adoption in this study based on the larger number of stakeholders involved in construction industry specifically in Klang Valley. A total of 50 questionnaires was collected from the stakeholders out of 100 distributed having a response rate of 50%. The respondent was reached through online distribution via various social media platform. The questionnaire was categories into 4 main sections namely respondent's demography, the implementation of cybersecurity system in construction digitalisation in Malaysia, potential threats to construction stakeholders and way forward to improve the implementation of cybersecurity in Malaysian construction. With the aid of Statistical Package for Social Science (SPSS) version 29, the data was analyse using descriptive statistic, regression analysis. After that, the finding and discussion conducted to come up with conclusions.

ANALYSIS AND FINDINGS

Respondents' background

This section from the questionnaire data collected through survey. Table 1 show the respondents data from various stakeholders involved in construction. The stakeholder's group was focuses mainly to the design team and IT department of the firm. Table 1 show the percentage of the respondents from the survey. The background of the respondents includes Quantity surveyors (18%), Engineers (26%), Architects (16%), Contractors (24% and IT department/Technical (16%). Most of the respondents (76%) are from private sector, 10% Government and Semi-Government respectively, 2% from MNC and GLC company respectively.

Implementation of Cybersecurity in Stakeholders' Company in Construction

The implementation of cybersecurity scrutinising the stakeholder company alongside with its measures. Table 1, it shows the implementation of cybersecurity system in stakeholders' company in construction.

Table 1. Mean score of Company Contribution Towards Implementation of Cybersecurity System in Construction

Implementation of Cybersecurity System	Average Mean	Ranking
Utilise software include any software that company use in planning, designing and costing	3.62	5
Aware of any cybersecurity threats	3.78	4
Implement cybersecurity measures such as use of anti-virus, regular software update etc	3.88	1
Able to faces any challenges in implementing cybersecurity measures in digitalisation construction	3.80	2
Have a future plan to avoid cyber security attacks such as continuous monitoring and auditing to detect anomalies, cybersecurity training or awareness, etc.	3.80	3

Source: Authors (2024)

Most of the respondents ranked "implement cybersecurity measures such as use of anti-virus, regular software update etc." as first ranked factors. This indicator has a high mean score of 3.88 as stakeholders in construction are mostly using computer in their daily task which this definitely increase the awareness among of them to implement the cybersecurity system. Most company will invest money to get a good anti-virus in protecting all the data which are vulnerable to cyber threats. According to Al Zaidy, (2014), the anti-virus is important thing to consider in protecting the information as if it is not implemented it cause the risk of being attack of the data increase. Agreed that invest in computer security and protection measures by using current anti-virus software and other measures to protect against malware. Plus, National Cyber Security Centre (2016), also stated that computer will experience the risk of data hacking if there is

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

no anti-virus which means stakeholder who use computer to complete work, which at least they should have anti-virus in their computer to protect the construction data such drawing design, financial report etc. It is a good sign that all stakeholders agreed that anti-virus was implemented in their company which this show that most of them are implement cybersecurity system during work. Meanwhile, stakeholders in the construction still do not really utilise software include any software that company use in planning, designing and costing. This is because the respondent came from different company, and they did the different role which means not every company will implement the use of software in completing the work.

Second and third rank with 3.80 mean score in implementing cybersecurity in construction is "Stakeholders able to faces any challenges in implementing cybersecurity measures in digitalisation construction" and "have a future plan to avoid cybersecurity attacks such as continuous monitoring and auditing to detect anomalies, to have a cybersecurity training or awareness". As stated by the National Security Council (2020), the government supports stakeholders to be involved in the advancement of the digitisation era. These days, a lot of construction operations are automated and make sure of sensors and smart devices. Cybercriminals might be able to manipulate these comprised systems to physically harm property. Which means this problem of lack of the implementation of cybersecurity system in stakeholders' company in construction will be settled as the Malaysian government currently invite all the stakeholder including in construction sector to enhance the use of technologies in their company to make sure the construction sector is increasingly advanced in technology management.

Potential threats of cybersecurity

Threats in cybersecurity easy to happen as it is because stakeholders of the construction industry currently uploaded all the important document in cloud computing as they used of big data to keep a lot of files that been contracting with the client. These threats can diminish the data or sell the data to the third party. Table 2 highlighted the potential threats which can interrupt cybersecurity activities in term of data, financial and performance aspects.

Table 2. Mean score on Potential Threats of Cybersecurity on Construction Stakeholders, In Term of Data, Financial and Performance Aspect

Potential Threats of Cybersecurity	Average Mean	Ranking
Data aspect		
The potential impact of cybersecurity threats, particularly in term of data, on the digitalisation of the construction project should be considered	4.02	1
Company has experienced cybersecurity incidents such as data breaches, related to digitalisation of the construction project	3.38	9
The cybersecurity threats affect the data breaches in digitalisation of construction projects in the aspect of designs, budgets, schedule on client detail	3.76	8
Financial Aspect		
Cybersecurity threats affect the financial aspects in digitalisation of construction projects (e.g., cost overruns, budget allocation)	3.82	5
Cybersecurity threats cause costs provision for remediation costs (e.g., invest for cybersecurity protection)	3.86	4
Cybersecurity threats causing a loss of productivity and revenue in terms of project workflow disruption	3.80	7
Performance Aspect		
Cybersecurity threats influence the reputation and trustworthiness of construction companies involved in digitalisation of construction projects	3.90	3
Construction company's industry reputation suffer because of a cyber security incident	3.80	6
Cyber security threats affect construction companies' intellectual property infringement	3/90	2

Source: Authors (2024)

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

Based on Table 2, potential threats of cybersecurity on construction stakeholders will interrupt the work process. Most of the respondent agreed that data aspect is more exposed to potential threats of cybersecurity on construction stakeholders which the potential impact of cybersecurity threats, particularly in term of data, on the digitalisation of the construction project should be considered which rank as first potential threats with a mean score of 4.02. The data in construction such as built-up rate, preliminary estimates, payment etc. is private and confidential to share or exposed to others. Mantha & De Soto (2019) agreed that data breaches happened especially to the stakeholders who are involved or working with the digitised world environment. The data breaches are easy happen so all new digital technologies required data security and protection tool in reducing the threat of data to ensure that there is no major risk of them happening in the future (Jennifer A. Beckage & Daniel J. Parziale, 2021).

The potential threats in cybersecurity in rank second 2nd and third 3rd are related to "Performance Aspects". Where, "Cyber security threats affect construction companies' intellectual property infringement" and "Cybersecurity threats influence the reputation and trustworthiness of construction companies involved in digitalisation of construction projects" with a mean score of 3.90 respectively. Moreover, the performance aspect also affected potential threats of cybersecurity on construction stakeholders which cyber security threats affect construction companies' intellectual property infringement. Jaafar et al., (2018), agreed that potential of threat also causes of hacked of intellectual property infringement. Intellectual property infringement such as project proposal, rate used in bidding of tender can be stolen by the hacker after they are able to enter to the place where important data is stored. So, the competitor can change or adjust their bidding rate to win in the project. When a company has been hacked, they panic so much that they are willing to do anything including exchanging property or money to pay the hacker who has allegedly told them that they have hacked the company (Farhat et al., 2017). All stakeholders should be more cautious about cybersecurity hazards as it can affect many things. Plus, the potential threats of cybersecurity on construction stakeholders will influence the reputation and trustworthiness of construction companies involved in digitalisation of construction projects. And at the end, the company will be corrupted because there causes no capability to protect the important data created.

Way forward towards cybersecurity usage among stakeholder and threats minimisation

There is improvement that could be made in promoting cybersecurity in digitalise the construction industry. Among others, there are three (3) categories that need to focus on namely Individual approach, Management approach and Government approach. These approaches are believed to strengthen the adoption of digitalisation by looking at the threat control and mitigation of cybercrime as shown in Table 3.

Based on Table 3, it shows the ways to improve the implementation of cybersecurity usage among stakeholders and minimise threats incidents in term of individual, management and government approach. The top three (3) approach is in the categories of "individual approach". The first potential ways to improve the cybersecurity implementation is by implementing a strong password. A strong password is required to be implemented in all digitalised technologies to protect the data. According to Al Zaidy, (2014), where all digitalised gadget and technology are mostly contained, and it is used as place to keep personal information data which means this digitalised gadget and technology is opening opportunities for cyber security threats to occur. So, the use of strong password is really important to ensure the possibility of hackers accessing the data is reduced (WaterISAC & Security Information Centre, 2016). Plus, Borky & Bradley, (2019) also add their opinion which the user should change the password frequently to avoid cybersecurity attacks and spread of sensitive information to others.

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

Table 3. Mean Score on Ways to Improve the Implementation of Cybersecurity Usage Among Stakeholders and Minimise Threats Incidents in Term of Individual, Management and Government Approach

Ways to Improve Implementation of Cybersecurity and Minimise Threats Incidents	Ranking	Average Mean
Individual Approach		
Implement strong password	1	4.44
Regularly update software and firmware	3	4.32
Back up data regularly and securely	2	4.36
Implement individual access control such as card usage for access	8	4.20
Management Approach		
Conduct cybersecurity awareness training for all employees	9	4.20
Conduct vulnerability assessments and penetration testing	10	4.18
Partner with cybersecurity professionals for guidance and support	7	4.24
SOP on incident response plan such as written backup plan in hardcopy manual	5	4.26
Government Approach		
Cybersecurity education and training	4	4.32
Provide a safe platform for information sharing and collaboration	6	4.24

Source: Authors (2024)

In addition, the second highest rank of average means of 4.36, is “back up data regularly and securely”. All the data involved in the construction which starts from pre-construction until post construction is very important as it will be used again during preparing of final account or maybe for audit purpose. Backup data is crucial for protecting against cybersecurity threats in construction which this was agreed by Parsola (2022), which the data must be always backup to minimise the loss of data. Alongside with the third rank with mean score 4.32 is “regularly update software and firmware”. The company should keep the updates with their software to ensures a preventative measure such as Firewalls, antivirus software, and automatic updates are tools that can be used to identify, stop, or neutralise cyberattacks from occurring (Kavak et al., 2021). Thus, construction companies are protected from unwanted access to important systems and data. In other words, this proactive strategy helps the companies in construction remain resilient overall in the face of changing cyber threats in addition to guarding against possible breaches. Therefore, whether a threat comes from outside the company or from within, a well-established cybersecurity program aids in identifying and mitigating it. Construction companies can mitigate the impact of cyber threats on project timelines and overall operations by promptly detecting and neutralising them through the implementation of incident response plans and continuous monitoring for unusual activities. This parallel to the García de Soto et al., (2022) research was conducted, where the participants give an opinion on cybersecurity which it can help to reduce risk as more of the foundational measures to reduce it.

Meanwhile the lowest rank of average means of ways to improve the implementation of cybersecurity usage among stakeholders and minimise threats incidents is through “management approach” which “conduct vulnerability assessments and penetration testing”. The vulnerability assessment takes time to conduct and not only certain people who are experts in this field can conduct this assessment. This assessment is actually really good as it can identify and evaluate security risks which definitely benefited to the construction stakeholders who conduct this assessment and test. The National Cyber Security Centre, (2016), state that everyone who connected to the network should do assessments of threat to identify either become victim or not. While Parsola, (2022) state that vulnerability assessment and penetration testing should always conduct to ensure that the weakness system can be found.

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

The ability to put preventive measures in place is one of the core components of cyber security. Firewalls, antivirus software, and automatic updates as previously mentioned, function as digital controllers, monitoring and managing inbound and outgoing network traffic. Program for cybersecurity is necessary to safeguard vital infrastructure (Glantz et al., 2016). Cyber security programs are essential to protect critical infrastructure in the construction industry due to the sector's growing reliance on digital technology. Construction projects are now more efficient due to the integration of Industry 4.0 pillars, but they are also more vulnerable to cyber threats. It is important to protect sensitive data, such as financial information for construction projects, project plans that are difficult to share with third parties and architectural designs sketched for construction, as any compromise can have adverse effects.

CONCLUSION

In a nutshell, based on the literature review and survey that have been completed, the implementation of cybersecurity system in the digitalisation of the construction industry in Malaysia are aware of the cybersecurity threat but not really in depth which this still considered as good sign of cybersecurity system. Currently the cybersecurity systems in construction industry are not widely implemented as it is not a major contributor to cyber security intrusions and threats. In lieu of that, the stakeholders are also handling their work using digitalised technologies which allow them to implement cybersecurity measures such as the use of anti-virus, regular software update etc., in their daily task by using digitalised gadget. In contrast to that, there are also certain stakeholders who are still not implementing cybersecurity system in the digitalisation of the construction, due to less IT literate or the company is not directly involved in mega project. In addition to that, factor of high investment in cybersecurity also a concern by the stakeholders as they worried if they cannot gain a profit from the investment. In term of potential threats of cybersecurity on construction stakeholders in Malaysia, the data aspect which the most contribute to the threats. As, data is the critical asset that needs to be protected, its exposure in the digitalised world creates a chance for threats to occur. The data aspect contributes to the most potential threats of cybersecurity on construction stakeholders because construction is complex which involves with large of data to handle for one (1) project. Plus, there is reason why data aspect is on the first rank of potential threats of cybersecurity on construction stakeholders. It involved many parties or stakeholder in completing of one (1) project. Alas, cybersecurity threats happen in construction which leave a bad impact where data and confidential information about construction projects are hacked for malicious use. Lastly, the implementation of cybersecurity usage among stakeholders can enhance and minimise the threats incidents through individual approach such as implementing strong password, regularly backup the data and update software and malware for the office gadget they use. The rationale behind this is because the individual is the person who is involved directly managing the data of the project in construction, so that person knows which data is to be kept private and which data can be shared to others. Construction involved many sensitive data which this a bit difficult to handle, hence, through individual approach this problem can be reduced. Each data handled then proposed strong password to make it secure and protected from cybersecurity threat. The data of construction project is always shared on cloud computer which opens the opportunity of threat and breaches of data to happen. As such, the construction industry still has large potential to the cybersecurity threat it may not happen aggressively now, but it will happen more severely as digitalisation technology advances. Due to the complexity of the construction industry, it is not easy to handle events where many stakeholders are involved.

ACKNOWLEDGEMENTS/FUNDING

The author greatly appreciates the support and contributions of several individuals and organisations that made this work possible. Special thanks to Universiti Teknologi MARA (UiTM), Shah Alam, for providing the facilities and resources essential for conducting this research. The authors also want to thank participants from the industry who directly involved in this research survey.

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

AUTHORS' CONTRIBUTIONS

Ramli Isa conducted the research, wrote and reviewed the article. Har Einur Azrin Baharuddin conceptualised the central research idea and provided a theoretical framework. Har Einur Azrin Baharuddin designed the research, supervised the progress of the research; Har Einur Azrin Baharuddin anchored the review, revised and approved the submission of the article. The third author, Airul Faizal Othman, assists in conducting the survey among the PWD's professionals.

REFERENCES

Al Zaidy, A. (2014). What are Cyber-Threats, Cyber-Attacks and how to defend our Systems. https://doi.org/10.13140/RG.2.2.30414.59208

Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345–404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10

De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Farhat, V., Mccarthy, B., Raysman And R., & Canale, J. (2017). Cyber Attacks: Prevention and Proactive Responses", *Practical Law*, pp. 1-12, 2011. Retrived from: http://us.practicallaw.com/3-511-5848.

Jaafar, M. A., Husni, H., & Yusof, Y. (2018). IR 4.0 Readiness: Big Data Sources, Issues and Challenges. *Journal of Social Science and Humanities, 1*(3), 2600–9056. https://doi.org/10.26666/rmp.jssh.2018.3.5

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. In Cybersecurity (Vol. 3, Issue 1). Springer Science and Business Media B.V. https://doi.org/10.1186/s42400-020-00050-w

Mantha, B. R. K., & De Soto, B. G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. 29–37. https://doi.org/10.3311/ccc2019-005

National Cyber Security Centre. (2016). Common Cyber Attacks: reducing the impact. Retrieved from: https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact

National Security Council. (2020). Malaysia Cyber Security Strategy 2020-2024. Retrieved from: https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

Parsola, J. (2022). Cybersecurity Risk Assessment and Management for Organizational Security. *NeuroQuantology, 20*(5), 5330. https://doi.org/10.48047/nq.2022.20.5.nq22815

Rossouw von Solms, & Johan Van Niekerk. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

https://doi.org/10.24191/bej.v21iSpecial Issue.1598

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *IJARCCE, 7* (11), 125–128. https://doi.org/10.17148/ijarcce.2018.71127

WaterISAC, & Security Information Centre. (2016). 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks. https://www.waterisac.org

https://doi.org/10.24191/bej.v21iSpecial Issue.1598