INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Adoption of Cyber Insurance in Malaysian Organisations

Nur Hidayah Abd Rahman, Rajeswari Raju*, Suriyani Ariffin & Nor Hasnul Azirah Abdul Hamid
Faculty of Computer Science & Mathematics
Universiti Teknologi MARA
Terengganu (UiTM)
Email: hidayahrah97@gmail.com, *rajes332@uitm.edu.my

Atif Ahmad
School of Computing & Information Systems,
University of Melbourne, Australia

Submitted: 26/8/2022. Revised edition: 20/9/2022. Accepted: 20/9/2022. Published online: 20/11/2022
DOI: https://doi.org/10.11113/ijic.v12n2.380

***Abstract*—As businesses have embraced more and more technology, cyber risk has become one of the essential components of a risk management initiative that seeks to mitigate and analyze the multitude of new risks. One risk mitigation process is investing in cyber insurance to safeguard the organisations' assets from cyber threats by transferring them to the insurer. For businesses to decide on cyber insurance, choosing the right insurance plan and policy is crucial. To do so, they need to consider the factors of its implementation. Therefore, this paper aims to investigate the adoption of cyber insurance in Malaysian organisations, thus further exploring the organisations' perceptions of the factors of adopting cyber insurance. A qualitative study is conducted to understand and describe Malaysian organisations' needs, obstacles, and processes related to cyber insurance adoption by interviewing cybersecurity professionals and cyber insurance personnel to explore valuable insight into the existing knowledge. 30% of the respondents have adopted cyber insurance. While 40% of the respondents were unsure, the other 30% did not adopt cyber insurance in their organisation respectively. These insights include the factors in adopting cyber insurance among Malaysian organisations, which might be crucial for informing future research and practice in the cyber insurance industry. The novelty of this research is the overview of knowledge gaps and perceptions related to the adoption of cyber insurance in Malaysian organisations. Also, this research aims to consider the advantages of the relevant obstacles that influence the decision makers to adopt cyber insurance.**

***Keywords*—Cyber Insurance, risk management, Malaysian organisation, cybersecurity**

I. INTRODUCTION

With a pandemic happening around the globe, cyber-attacks have increased. They are effectively used as a weapon against countries due to the dominance and extensive growth of dependency on cyberspace. Despite the necessity of having security measures, some organisations are reluctant to enrol in such policies and are willing to risk substantial cyber damage caused by attackers [5].

In Malaysia Cyber Security Strategy 2020 - 2024, the authors analysed that the Royal Malaysia Police had to deal with 10742 cases related to cybercrime, with an estimated loss amounting to almost RM400 million in 2018. In just one (1) year, in 2019, the number has increased to 11875 cases with an estimated loss of nearly RM500 million. Fig. 1 displays the cybercrime statistics in 2018 & 2019 [6].

Basyir supports this statistic, that stated a statistic from Malaysian police had reported an increase of 5,416 (24.7 per cent) cybercrime cases recorded between 2019 and last year, which makes a total of 67,552 cybercrime cases reported from 2007 until June 20 this year [1]. With the increase of cases, it has become evident that the reliance on digital technology during this pandemic not only created new opportunities but also opened the floodgate of risks and vulnerabilities to the economic growth of this country. The numbers are shocking for economic gain, and it is not an issue that a country can solve alone as it is a borderless, sophisticated, and complicated risk [6]. Therefore, it has become one of the government's main focus areas to clamp down on cybercrimes to accelerate economic growth.

In his article "Cybersecurity: Staying Ahead of Cybercriminals", Yun explained that the digital products focused on speed and convenience had been developed by financial institutions creating additional points of vulnerability that fraudsters could exploit online [7].

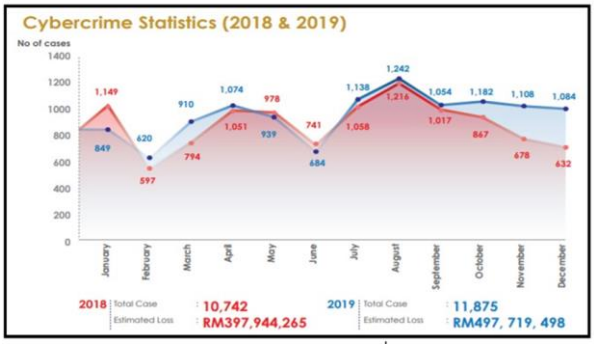

Fig. 1. The cybercrime statistics (2018 & 2019)

Fig. 2 shows the most challenging factors in expanding new digital products in Malaysia by global fraud specialist GBG, demonstrating the highest fraud prevention for new digital products [7].

The Movement Control Order (MCO) in 2020 presented the critical importance of adaptiveness for business resiliency and revenue growth that highlighted the response to business and market changes, increasing the ability to innovate and accelerating the shift to digital business [1].

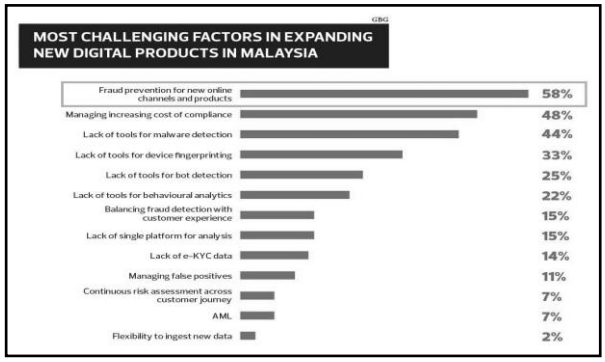

Fig. 2. The most challenging factors in expanding new digital products in Malaysia

However, with a shot up of 82.54% cybercrime according to a report by GBG during this pandemic [8], along with the highest challenging factors in expanding the new digital products in Malaysia [7], it might lead to the struggle of businesses in their digital transformation journey. Moreover, Abrar A. Anwar, the managing director and Chief Executive Officer (CEO) of Standard Chartered Malaysia, says that the surge in the pandemic has led to a significant increase in cyber threats that have become key challenges in securing the digital transformation throughout Asia, which remains behind on adopting the security frameworks [8].

II. LITERATURE REVIEW

Information Technology (IT) can play a significant role in empowering industries to meet their strategic objectives. In this case, organisations may have to increase their investment in IT to remain competent, innovative, and agile [9]. However, it is neither impossible nor economically feasible to protect organisations against all vulnerabilities [10]. Eventually, organisations that adopt cyber insurance as risk management need to understand the risks they might face and how cyber insurance can reduce them [10].

As reported in "A Probabilistic Analysis of Cyber Risks", it is difficult to prioritize the security investments such as encryption software, anti-phishing training, and upgrading network equipment that are measured by cyber-risk management given the doubts and the charges involved [8]. However, Dambra *et al*. claimed that cybersecurity investment takes about half of the spending on equipment as a precaution against the organisations' assets from cyber threats [11]. Due to the high expenses in cyberspace, some organisations have become progressively technology-dependent and highly threatened by the risks of cyber-attacks and data breaches. Since most organisations cannot endure massive damages that might cause huge losses, they adopt cyber insurance by transferring the financial risks related to network and computer incidents to a third party known as the insurers, which aim to mitigate the cost of cyber threats [11]. The consequences of not practising risk management would result in poor control and managing cyber threats.

A. Cyber Insurance

Cyber insurance is emerging as an effective means to defend organisations against future cyber-attack-related losses [12]. However, the cyber insurance process involves two key players: a first supply-side entity that provides insurance to the organisation, especially the insurance company called an insurer and a second demand-side entity that buys the insurance, known as the insured [11].

Cyber insurance is still a new concept in practice and research throughout Southeast Asian countries, and there are many unanswered questions regarding its adoption, especially in Malaysia [1]. Cyber insurance is believed to be an essential mechanism to protect organisations from cyber-attack that can result in data and reputation loss, thus impacting the organisation’s bottom line [12][18][19]. A recent review of the literature on this matter found that cyber insurance plays a vital role in minimizing potential losses in an organisation by mitigating the risks caused by cyber threats [18]. Fig. 3 compares the product coverage provided by insurance companies in Malaysia.

Cyber Insurance Services / Coverage	Chubb	Tokio Marine	AIG	Howden	MSIG
Business interruption loss (e.g: human errors, network security failure etc)	✓	✓	✓	✗	✓
Data loss	✓	✗	✗	✗	✓
Business interruption event (e.g: delay, disruption, and acceleration costs)	✓	✓	✓	✓	✓
Crisis management event costs	✓	✓	✗	✗	✗
Cyber liability	✓	✗	✓	✗	✓
Cyber extortion	✓	✓	✓	✓	✓
Online media liability	✓	✗	✓	✗	✓
Regulatory investigations expenses	✓	✓	✗	✓	✓
Loss of digital assets	✗	✓	✗	✗	✗

Fig. 3. Cyber insurance product coverage

Most insurance companies provide different product plans at different prices. This, however, has contributed to the misinterpretation and misunderstanding among insurers and policyholders. Such a misleading assumption can lead to critical consequences regarding the difficulty in comparing the values and prices for buyers [12].

However, the majority of the businesses do not satisfy with the existing cyber insurance products because it doesn't meet their expectations and needs. As mentioned by Ikeda in a survey of cyber insurance policyholders, only 26% had updated the coverages. In comparison, 55% were interested in the new cyber insurance model, including data loss, denial of service, and cyber extortion [20].

As mentioned by Uuganbayar *et al*., the risk assessment is the base part of evaluating cyber insurance quality [13]. In most cases, the quality is computed unfairly due to the lack of a model or practical result for calculating the possibility of an attack; with the increase of time, the visibility of unknown vulnerabilities in the system also increases, as assumed. The key to finding the possibility of attack and offering acceptable quality cyber insurance to the organisation is to address this issue to define the required time [13].

B. Factors that Influence the Adoption of Cyber Insurance

National Cyber Security Agency (NACSA) has listed Malaysian Cyber Laws on its official portal, as portrayed in Table I. There is no indicator for Malaysian organisations to comply with any related laws when they adopt cyber insurance. This demonstrates that cyber insurance is never precisely considered a form of governance in Malaysia [14].

TABLE I. MALAYSIAN CYBER LAWS

Law	Purpose
Copyright (Amendment) Act 1997	To make better provisions in the law relating to copyright and for other matters connected in addition to that.
Computer Crimes Act 1997	To provide for offences relating to the misuse of computers.
Digital Signature Act 1997	To make provision for and regulate the use of digital signatures and provide for connected matters.
Telemedicine Act 1997	To provide for the regulation and control of the practice of telemedicine and for matters connected in addition to that.
Communications and Multimedia Act 1998	To provide for and regulate the converging communications and multimedia industries and incidental matters.
Electronic Commerce Act 2006	To provide for legal recognition of electronic messages in commercial transactions, the use of the electronic messages to fulfil legal requirements.

However, the Malaysian Communications and Multimedia Commission (MCMC) has published the Technical Code under the Communications and Multimedia Act 1998, which entails the prerequisite for network interoperability and the advancement of security of network services [4].

The Technical Code outlines a new approach as a risk treatment to resolve the cyber security incident within the Malaysian organisations' security risk management background. Also, they have highlighted that cyber insurance does not reduce the possibility of cyber security risks that are being mitigated [4].

With additional guidance from several security standards, guidelines and frameworks that the Malaysian government has implemented, such as MS ISO/IEC 27001:2007 or ISO/IEC 27001:2005 for the implementation of enterprise-wide Information Security Management System (ISMS) [2], Cyber Security Framework for public sector (RAKKSSA) [3], as well as Technical Code for Information and Network Security (Cyber Insurance Acquisition) which is registered by Malaysian Communications and Multimedia Commission (MCMC) [4], the gaps can be identified where qualitative study should be conducted to gain more perspective and a broad overview from the selected representatives in Malaysian organisations.

To successfully implement cyber insurance in an organisation, this study needs to address the challenges and issues organisations must deal with when implementing cyber insurance. Moral hazards, lack of historical data, the inability to predict the cyber risk future, businesses not being aware of what is covered in the complicated written policy, adverse selection, significant cascading loss events, and legal battles over fundamental issues. A moral hazard occurs when there is asymmetric information between two parties and a change in the behaviour of one party that might occur after an agreement between the two parties is reached. On the other hand, adverse selection refers to a situation where the insurers have more information than the insured, or vice versa, in some aspect of product quality, insurance policy and any other related information that might lead to exploitation from one party. These challenges and issues need to mitigate fully because the future growth of the implementation of cyber insurance will depend upon how these issues and challenges are resolved.

C. Significance of Cyber Insurance

As monitoring cybersecurity posture is highly complicated, cyber insurance has been an essential component that seeks to mitigate and analyse the horde of new risks. Companies that purchase cybersecurity insurance today are considered early

adopters. According to the Technical Code prepared by the Malaysian Communications and Multimedia Commission in Guidance of Malaysia Communications and Multimedia Act 1998 under Section 184, "the adoption of cyber insurance is to reduce the impacts of a cyber incident that shall be organisation shall consider to information security controls as part of effective risk management and risk treatment approach" [4].

In the wake of numerous recent cyber-incidents, cyber insurance has experienced a spike in demand as it can be a valuable risk transfer mechanism that can protect the financial shock of businesses. Investing in cyber insurance or cyber liability insurance is one of the risk mitigation processes to defend against damages from cyber threats by shifting such risks to another party known as the insurer. Most insurers will provide a focused set of coverage that is cost-effective to the businesses, as well as additional services such as access to the IT forensic specialist, who can help in advising on the appropriate procedures during and after the cyber-incident.

However, cyber insurance is still in its infancy, especially in Malaysia, because of limited cyber insurance coverage options due to the lack of standardised cyber risk assessment and potential misunderstanding between an insurer and an insured [5]. Raju *et al*. have conducted research among university students to explore the student's awareness and knowledge of cyber security, cyber-attack, and cyberbullying. The finding shows that tertiary students still lack this knowledge [22]. So, early education awareness about cyber insurance should be given to educating individuals early.

This is where having the correct information about cyber insurance and the risk intelligence information might help organisations, especially small and medium-sized enterprises (SMEs), direct their security efforts and budget correctly by selecting a proper cyber insurance liability.

The novelty of this paper and is interrelated to the past research is the overview of knowledge gaps related to the adoption of cyber insurance in Malaysian organisations. Additionally, this paper also aims to consider the advantages and relevant challenges that influence the decision to adopt cyber insurance. A qualitative study will be conducted to understand and describe Malaysian organisations' needs, obstacles, and processes related to cyber insurance adoptions.

III. METHODOLOGY

As for this study, the qualitative method is used, where in-depth interviews are being conducted with open-ended questions given to the interview. The Etiquette Committee approves the list of questions in the questionnaire for the interview committee of the researcher organisation that carries out this study. Given that this study aims to explore the adoption of cyber insurance in Malaysian organisations along with the key factors and challenges affecting the adoption, a diverse group of professionals from various stages of the cyber insurance process have participated in this interview. These individuals were based in Malaysia and have engaged with cyber insurance portfolios in their current companies in Malaysia. A pre-prepared questionnaire is used in the interview session, but the interviewee can react openly in their words. According to Zikmund, open inquiries in in-depth interviews will help respondents clarify and state their perspectives without being restricted by biased classifications or the need to answer the rigid questions provided [15].

Each interview session is recorded to allow the transcription process to occur, thereby providing a richer pool of data for analysis to be carried on. For the data analysis, a thematic analysis approach is adopted that strives to identify patterns of themes, weeding out biases and establishing the overarching impressions of the collected interview data. Based on Nurse *et al.*, the thematic data analysis approach is an excellent way to analyse the interview data by identifying its keycodes, especially the discrete information communicated in the data, and from the codes, construct the themes that can draw out the essential findings and form conclusions to the research [16].

IV. FINDINGS

Overall, this study examines the adoption of cyber insurance in Malaysian organisations in the mainstream focusing on the cyber insurance adoption in Malaysian organisations by using thematic analysis.

A. Cyber Insurance Adoption in Malaysian Organisations

In Malaysia, implementing cyber insurance is still a considerable gap among organisations. Unlike any other insurance product purchased by default due to financial obligations, many organisations in Malaysia are still lackadaisical towards cyber insurance [17]. We have interviewed ten (10) representatives from different backgrounds of organisations which are presented in Table II.

TABLE II. ORGANISATIONS' BACKGROUND

Respondent	Background		
	Adopt cyber insurance	***Industry***	***Years of operation***
1	Yes	Information Technology	More than 10 years
2	Yes	Telecommunication	More than 10 years
3	Yes	Manufacturing	More than 10 years
4	Not sure	Banking	Not Applicable
5	Not sure	Telecommunication	More than 10 years
6	Not sure	Information Technology	Not Applicable
7	Not sure	Manufacturing	More than 10 years
8	No	Cybersecurity provider	6 – 10 years
9	No	Recruitment	Less than 3 years
10	No	Information Technology	More than 10 years

Of the initial cohort, three (3) representatives have adopted cyber insurance. At the same time, the rest of the respondents were not sure (40%) and did not adopt cyber insurance (30%) in their organisation respectively.

B. Thematic Analysis

Based on the findings in Table II, further analysis was carried out to identify the factors that influence the decision organisations' decision to adopt cyber insurance was conducted by using NVivo 12 Plus, where we used a coding feature to classify themes in the transcribed dialogue from the interviews Based on their comments, several overarching themes are identified in Table III.

TABLE III. THEMES OF THE FACTORS

Item	Theme	Number of coding references
1	Financial impact	18
2	Lackadaisical attitude	32
3	Lack of evidence and successful adoption	14
4	Lack of standards and policy	32

As analysed in Table III, items 2 (lackadaisical attitude) and 4 (lack of standard and policy) have the highest number of coding references. Most respondents frequently mentioned those as the benchmark in their organisations' decision-making for cyber insurance adoption.

1) Lackadaisical attitude

The majority of the respondents pointed to a lackadaisical attitude and the corresponding ability to the importance and advantages of adopting cyber insurance. Respondent 7 stated:

"Most of the employees lacked knowledge of cybersecurity and cyber risk awareness. This is my first time knowing the existence of the cyber insurance industry."

Respondent 8 also mentioned:

"Usually, the authorities such as Cybersecurity Malaysia (CSM) or National Cyber Security Agency (NACSA) will be approached by local organisations when cyber incidents have already happened. Many organisations are less likely to believe or expect it to happen."

As anticipated, it is plausible that several limitations could have influenced the organisations to protect themselves from the breaches. The lack of knowledge and understanding of cyber insurance options have acted as critical factors for cyber insurance adoption. This is expected as in the findings (Table II), most Malaysian organisations were not adopting cyber insurance as they had no idea about their cyber risk exposures to assess the type and coverage of insurance they need.

2) Lack of standard and policy

According to Respondent 1, Malaysia does not have proper guidance or regulations on cyber insurance; therefore, most organisations tend to oversubtle when it comes to insurance policies. He added:

"I think Malaysia doesn't have sufficient maturity to develop a proper cyber insurance policy, especially for small and medium-sized enterprise (SME) companies."

Besides, the lack of awareness of cyber insurance coverage leads to many organisations overlooking that data privacy breaches are included in the range. This confirms that there are standards and policies in preparing the coverage. Respondent 5 agreed and said:

"It is difficult to determine what to include in the coverage if we plan to adopt the cyber insurance."

Respondent 6 added:

"Many organisations may be unsure of what they need and what they are getting in the policies. Hence, they took every coverage they thought needed, which caused the premiums to be expensive."

There is a lack of standardization related to coverage and terminologies. Policyholders and insurers lack consensus regarding cyber breach costs covered by a policy. It might be an illegal and anti-competitive practice to share an agreed standard policy that causes the insurers' concern and is arguably against standard wording [21].

3) Financial impact

Financial impact also can be one of the factors that influence the decision-makers in adopting cyber insurance. Lack of knowledge of the coverage and product plans could lead to the high cost of cyber insurance premiums. Respondents 8 and 10 believed that it is not easy to find greater clarity on the specific products to achieve the agreement between the insurer and the insured. Respondent 10 explained:

"It is difficult to present the product plans to our board of directors because most of the time they will question the return on investment (ROI) for subscribing to cyber insurance premium."

Respondent 5 expressed that the reluctance to subscribe to cyber insurance is due to the high cost of cyber insurance premiums. He added:

"One of the fear factors is the cost that an insurance provider will charge to Malaysian organisations. Only large companies can afford to pay for the expensive cyber insurance premiums because it is quite substantial."

The potential financial implications of cyber breach exposures are huge. They may not realize the need for cyber insurance when they only face smaller cyber-attacks. On the other hand, the organisation's decision-makers face institutional pressures for legitimacy from stakeholders that often require increasing profitability.

4) Lack of evidence and successful adoption

Based on the respondents' comments, adopting cyber insurance in Malaysia today is extremely rare. This is revealed by Respondents 6 and 9 that Malaysia's regulations still lack legal precedent on cybersecurity issues. Respondent 6 claimed:

"To my knowledge, there is less case law on cyber insurance in Malaysia. Thus, the buyers are more concerned about having to litigate a disputed claim due to disagreements over the policy coverage."

Respondent 4 supported this by saying:

"Not all local banks have practised local guidelines from Bank Negara Malaysia (BNM). Instead, some banks are regulated by Monetary Authority of Singapore (MAS) guidelines because the main headquarters are mostly in Singapore."

In this case, regulations are supposed to act as a driving force in the evolution of common norms and standards [12]. To support the adoption of cyber insurance, government agencies and the insurance industry should work together to develop underwriting practices that reduce cyber risks and promote risk-based pricing. A guideline would help decide the types of damages covered in cyber insurance.

V. CONCLUSION

Cyber-attacks involve massive costs, which can neither be quantified nor qualified easily. Cyber insurance is one of the methods and practices in Cyber Security Risk Management to ensure the vulnerability or attacking data is managed and protected. To fully mitigate the dynamics of cyber-attacks, cybersecurity, one of the pillars of National Policy in Industry 4.0, plays a vital role so that organisations in Malaysia can protect their data and technology in the industry. Terms of the cyber insurance impact on Malaysia's economy are difficult to measure due to various elements and parties involved. Thus, it is a significant activity that should not be overlooked.

Fully adopting cybersecurity in the industry relates to cyber insurance implementation, which is a part of Cyber Security Risk Management. This hyper-connectivity is a powerful tool that is an opportunity for growth in both public and the private sectors, whether for government, business or Small and Medium Industries (SMEs).

Large organisations with stable economic positions can survive those cyber-attacks with their expensive cyber-defence technologies and capabilities. However, for SMEs that cannot afford the costly cyber-defence technologies and capabilities, cyber insurance is one option that they can implement to help them fine-tune their risks and aid in regaining business sustainability. This is due to the coverage insurance covering their losses against the cyber-attacks, thus allowing them to survive the complex and evolving threat landscape.

Consequently, the development and implementation of cyber insurance in this current advent of technologies might make it an essential component of Malaysia's economy and the diffusion of emergency and strategic services.

ACKNOWLEDGEMENT

Research Collaboration Fund (RCF) 2020, UiTM Terengganu, for funding this study, Malaysian Communications and Multimedia Commission for the reference of their Technical Code on Cyber Insurance and Cyber Security Malaysia.

REFERENCES

[1] Basyir, M. (2021, July 16). Malaysians Suffered RM2.23 Billion Losses from Cyber-Crime Frauds. New Straits Times. https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds.

[2] MITI. (2021). Ministry of International Trade and Industry Official Website of Department of Standards Malaysia, retrieved on June 10 2021, https://www.jsm.gov.my/ms-iso/iec-27001-2007-information-security-management-systems#.YMcheagzbD5.

[3] The Malaysian Administrative Modernisation and Management Planning Unit. (2021). Cyber Security and Disaster Response and Recovery, retrieved on June 10 2021, https://www.malaysia.gov.my/portal/content/30090.

[4] MCMC MTSFB TC G020. (2019). Technical Code Information and Network Security - Cyber Insurance Acquisition retrieve on June 10 2021. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G020_2019-INS-Cyber_Insurance_Acquisition.pdf.

[5] Vakilinia, I., & Sengupta, S. (2019). A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, 14(6), 1526-1538. https://doi.org/10.1109/tifs.2018.2881694.

[6] Malaysia Cyber Security Strategy 2020 – 2024. (Malaysia Cyber Security Strategy 2020 - 2024, 2020), retrieved on June 11 2021.

[7] Yun, T. Z. (2021, 22/03/2021). Cybersecurity: Staying Ahead of Cyber Criminals. The Edge Malaysia, https://www.theedgemarkets.com/article/cybersecuritystaying-ahead-cybercriminals.

[8] Pate-Cornell, M. E., & Kuypers, M. A. (2021). A Probabilistic Analysis of Cyber Risks. *IEEE Transactions on Engineering Management*, 1-11, https://doi.org/10.1109/tem.2020.3028526.

[9] Kamran Abbasi, N. P., Amin Hosseinian-Far. (2021). Centralized IT Structure and Cyber Risk Management. https://dx.doi.org/10.1007/978-3-030-68534-8_22.

[10] Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). Using Cyber-Insurance as a Risk Management Strategy Knowledge Gaps and Recommendations for Further Research.

[11] Dambra, S., Bilge, L., & Balzarotti, D. (2020). SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap.

[12] Kshetri, N. (2020). The Evolution of Cyber-insurance Industry and Market: An Institutional Analysis. *Telecommunications Policy*, 44(8), 102007. https://doi.org/https://doi.org/10.1016/j.telpol.2020.102007.

[13] Uuganbayar, G., Massacci, F., Yautsiukhin, A., & Martinelli, F. (2019). Cyber Insurance and Time-to-Compromise: An Integrated Approachx.

[14] Malaysian Cyber Laws. (2021). https://www.nacsa.gov.my/legal.php.

[15] Zikmund, W. (2015). Business Research Methods. 16th ed. Fort Worth, TX: Dryden.

[16] Nurse, J. R. C., Axon, L., Erola, A., Agrafiotis, L., Goldsmith, M., & Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1-8.

[17] Adnan Rizal Haris, Suhaimi Sarijan & Norhayati Hussin (2017). Information Security Challenges: A Malaysian Context. *International Journal of Academic Research in Business and Social Sciences*, 7(9), 397-403.

[18] Aziz, B., Suhardi, & Kurnia. (2020). A Systematic Literature Review Of Cyber Insurance Challenges.

[19] Mbatha, N. S. (2020). Factors Influencing Cyber Insurance Adoption in the South Africa Industry.

https://wiredspace.wits.ac.za/bitstream/handle/10539/30071/Final_Research%20_%20Report_MMDB_2019_2020_NS%20MBATHA%20-%202261524%20-%2004%20November%202020.pdf?sequence=1

[20] Ikeda, S. (2019). New Report Indicates Cyber Insurance Providers are too Slow to Respond to Emerging Threats, Customer Needs. https://www.cpomagazine.com/cyber-security/new-report-indicates-cyber-insurance-providers-are-too-slow-to-respond-to-emerging-threats-customer-needs/

[21] Neil, H.-B. (2019). Confusing Terminology Stunts the Growth of Cyber Insurance. *Computer Fraud & Security*, 2019(4), 16-17.

[22] Raju, R., Abd Rahman, N. H., & Ahmad, A. (2022). Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution. *Asian Journal of University Education*, 18(3), 756-766. https://doi.org/10.24191/ajue.v18i3.18967.