International Journal of Social Science Research
ISSN 2327-5510
2024, Vol. 12, No. 1

Cyber Insurance in Malaysian Organisations: An Introductory Journey

Rajeswari Raju (Corresponding Author)
Universiti Teknologi MARA (UiTM), School of Computing and Mathematics, Terengganu Branch, Kuala Terengganu Campus, 21080 Terengganu, Malaysia
E-mail: rajes332@uitm.edu.my
Nur Hidayah Abdul Rahman
Universiti Teknologi MARA (UiTM), School of Computing and Mathematics, Terengganu Branch, Kuala Terengganu Campus, 21080 Terengganu, Malaysia
E-mail: hidayahrah97@gmail.com
Sritharan Sangaran
PETRONAS Chemical Olefins Sdn Bhd, 24300 Kertih, Terengganu, Malaysia
Universiti Teknologi Malaysia (UTM) 81310 Skudai, Johor, Malaysia
E-mail: sritharan78@gmail.com
Sharifah Nurulhikmah Syed Yasin
Universiti Teknologi MARA (UiTM), School of Computing and Mathematics, Terengganu Branch, Kuala Terengganu Campus, 21080 Terengganu, Malaysia
E-mail: nurulhikmah@uitm.edu.my
Zeti Darleena Eri
Universiti Teknologi MARA (UiTM), School of Computing and Mathematics, Terengganu Branch, Kuala Terengganu Campus, 21080 Terengganu, Malaysia
E-mail: zetid415@uitm.edu.my

Received: August 10, 2023 Accepted: Sep. 30, 2023 Published: Nov. 22, 2023
doi:10.5296/ijssr.v12i1.21241 URL: https://doi.org/10.5296/ijssr.v12i1.21241

Abstract

Over the past century, many profound technological, economic, and social transformations have occurred. 21st century emerged as of technology and the borderless world; businesses have embraced more strategic ways to handle risk in computing; Cyber Risk Management (CRM) has become one of the essential components in risk management initiatives that seek to mitigate and analyse the multitude of new risks. One risk mitigation process is investing in cyber insurance to safeguard IT assets from cyber threats by transferring such risks to another party known as the insurer. However, implementing cyber insurance in Malaysia is still a considerable organisationsal gap. Unlike any other insurance purchased by default due to financial obligations, many organisations in Malaysia are still lackadaisical towards cyber insurance. The research looks into the factor that contributes to the gap. The study starts with identifying the research background and problem statement and then collecting the data. 30 semi-structured interviews were conducted. The data was collected from 30 experienced Malaysian organizations in the public and private sectors. Finally, the outcome is analysed and concluded.

Keywords: Cyber Insurance, Risk Management, Malaysia organization

1. Introduction

With ineffective cybersecurity policies and varying data protection regulations, the cyber insurance space in the Asia Pacific region could surge in the coming years, with organizations trying to understand the risk of the growth in cyber-attacks (Sriram, 2021). With the abundance of sensitive information now accessible, many firms are exposed to various cyber threats, from data theft and ransomware to corporate espionage, often without their knowledge (Yan, 2022).

1.1 New Law to Boost Cybersecurity

As published online in New Straits Times (Malaysia newspaper) on 15 Jun 2023, Prime Minister Datuk Seri Anwar Ibrahim said quote, "Malaysia is drafting a new law to bolster the country's resilience and response to cyber threats. The drafting of the new legislation was agreed upon with the National Cyber Security Committee. The unity government would not compromise with any attempt to undermine the country's cybersecurity" unquote.

The National Security Council's National Cybersecurity Agency, or NACSA, will be the leading agency to mobilise efforts across government agencies and industries to enhance Malaysia's cyber resilience. According to the news, the new law would provide NACSA with clear legal jurisdiction and authority to protect the country's cybersecurity and carry out enforcement. The Malaysian government will also streamline the role of entities related to cybersecurity to maximise efficiency and avoid overlapping functions to boost the country's cybersecurity (Adib Povera, 2023).

1.2 Cyber Security

Currently, 4.7 million experts worldwide are working in cybersecurity, trying to limit the global costs of cybercrime. These are expected to surge in the next five years, rising from US$ 8.44 trillion in 2022 to approximately US$ 11 trillion in 2023 and potentially reaching approximately US$ 24 trillion by 2027. However, as predicted by the Cybersecurity Workforce Study, a skills shortage still exists, with a gap of 3.4 million cybersecurity workers needed to protect organisations adequately, and this gap will not be closed in the near future.

2. Problem Statement

The trend of cyber-attacks is increasing daily as more people adopt digitalisation in their daily business, making them more exposed.

Malaysia is the second-highest Southeast Asian country that has seen a surge in web threats targeting businesses in 2022, with a 197% increase year-on-year, according to the latest data from Kaspersky. Kaspersky stated that Singapore logged the highest year-on-year jump in cyber-attacks on businesses last year. It recorded more than a three-fold spike (329%) after its business solutions blocked 889,093 web attacks, a whopping increase from 2021's 207,175 incidents (Sunday Daily Kaspersky, 2023).

Cyberspace is a constantly growing global digital network that associates several facets of life, including business and infrastructure. As the information technology role has evolved into a primary need for most organisations in Malaysia, new threats have been identified recently in

the news, including the most substantial ransomware attacks that hit businesses globally. With the growing number of emergent cybersecurity threats, organizations strive to carry on with the fast-changing threat landscape, involving several expert cybersecurity specialists (Sohime et al., 2020).

Based on a report from Symantec Corporation (2019), most of the large businesses in Malaysia have experienced a cyber-attack, and an average of 3.6% of the businesses experience successful attacks. Even smaller businesses are becoming increasingly vulnerable to targeted attacks. Based on the estimation in the Symantec Corporation (2019) report, about 60% of small businesses are closed within six (6) months due to a cybersecurity breach, as reported on the Internet Security Threat Report (ISTR, 2019).

3. Significance of the Research

To society:

A better understanding of the significance of adopting cyber-insurance. In the IT field, institutions' demands and needs can be enhanced with an appropriate data analytics approach in measuring the reliable factors of adopting cyber insurance.

To Industry:

As a guideline in deciding to adopt cyber-insurance, which includes considering the validity, compliance, cost, and usefulness.

4. Challenges

When the world moves toward the digital era, one will face the challenges of digitalisation, cyber security, and associated risk (Raju et al., 2022). To successfully implement cyber insurance in an organisation, it is essential to address the challenges and implemented issues that the organisations need to deal with when implementing cyber insurance. Many researchers have highlighted four (4) significant categories of cyber insurance challenges: barriers related to the cyber insurance product, risk, the insurer, and the regulation (Deloitte Insights, 2020).

The barriers associated with the cyber insurance product, unclear coverage, and cost of coverage in cyber insurance are the main reasons for the insured to implement cyber insurance (Pavel, 2020). On the other hand, the OECD (2017) report stated that in terms of barriers related to risk, it is concerned about the uncertainty of the extent of risk and the evolution of the system, resulting in cyber-attacks evolving. Another barrier to cyber insurance implementation is the insurer's barriers due to insufficient historical data to build predictive models and lack of experience and standardisation in cyber insurance policies (OECD, 2023). Regarding the regulation barrier, the current legal landscape is in flux without a transparent or standardised government policy, whether in cybersecurity or cyber insurance, and the regulation's complexity across the different states.

5. Literature Review

5.1 National (Malaysia)

There has been a rapid rise in Malaysia's small and medium-sized enterprises (SMEs) of successful cybersecurity breaches, where 60% of them are closed within six months, according to Internet Security Threat Report (ISTR, 2019). This lack of transparency in policies and practices has become a significant obstacle hindering cyber insurance adoption (Romanosky, 2019).

Cyber risks are growing exponentially due to digitisation and increasing technology dependence for businesses today. Based on a report by Cybersecurity solutions provider Fortinet, Feb 2023, Malaysia experienced an average of 84 million cyber-attacks every day during the fourth quarter of 2022 (Bernama, 2023). According to Fortinet Southeast Asia and Hong Kong vice-president Peerapong Jongvibool, the attacks included viruses, botnets, and exploits. The cyber threats in Malaysia registered 61.1 million virus detections, 50.2 million botnet attacks, and 7.5 billion exploit detections throughout the fourth quarter of 2022, compared with 200 billion attacks per day recorded globally (Fortinet, 2023).

5.2 International

On 26 Jul 2023, the U.S. Securities and Exchange Commission (SEC) voted 3-2 to adopt final rules that are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (including foreign private issuers). Specifically, the SEC's amendments require (Skadden, 2023):

- Current reporting of material cybersecurity incidents.
- Annual reporting of company processes for identifying, assessing, and managing material risks from cybersecurity threats; management's role in determining and managing the company's material cybersecurity risks; and the board's oversight of cybersecurity risks.

5.2.1 Key Requirements of Cybersecurity Incident Disclosure Rules (Skadden, 2023)

a) Disclosure within four business days after a company determines that a "cybersecurity incident" experienced by the company is material.

b) In the event disclosure is triggered, a company must describe:

- The material aspects of the incident's nature, scope, and timing.
- The material impact or reasonably likely material impact on the company, including its financial condition and results of operations.

c) Delay Due to Risks to National Security or Public Safety

A company may delay disclosure of a material cybersecurity incident for up to 30 days if the disclosure poses a substantial risk to national security or public safety. The disclosure may be delayed for an additional period of up to 30 days if the authority determines that disclosure

continues to pose a substantial risk. In extraordinary circumstances, in the case of risk to national security, disclosure may be delayed for a final additional period of up to 60 days.

5.2.2 Cybersecurity Risk Management, Strategy and Governance Disclosure (Skadden, 2023)

a) Whether and how the described processes have been integrated into the company's overall risk management system or processes.

b) Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes.

c) Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with using third-party service providers.

6. Cyber Space

6.1 Cyberattacks

It will be increasingly accelerated by key technology trends such as artificial intelligence like ChatGPT, the so-called “metaverse”, and the expanding worlds of IT, the Internet of Things (IoT), and operational technology (OT). In this context, awareness, understanding, and preparation are vital to prepare ourselves to overcome the attacks.

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 (Abd Rahman, 2022).

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 (Abd Rahman, 2022). The need for robust cyber-security in the banking sector is more critical today than ever.

While banks of the past defended themselves from malicious actors with better vaults, exploding dye packs, and armed guards—today’s banks face a very different breed of criminals. A study conducted by Cisco indicated that In Asia Pacific, many companies receive up to 10,000 daily threats, equating to 6 threats received every minute (EIOPA, 2019).

6.2 Cyber Risk Assessment

Businesses understand the spread of cyber risk by accessing varied services and assessing the holistic impact on the more excellent network (Sriram, 2021). Based on expert judgments, qualitative risk assessments using internal data can also be performed as self-assessments and, in a minor scope, on quantitative models (EIOPA, 2019).

According to Herr, the occurrence of active, adaptive challenges must be measured in cyber risk assessment in addition to an organisation's susceptibility to the outcomes of an event (Herr, 2021)

Besides the consequence-driven and threat-driven approaches, Alwi and Zainol Ariffin claim another approach in their studies, “Information Security Risk Assessment for the Malaysian

Aeronautical Information Management System," called ISO 27005's approach (Alwi, 2018). International Organization for Standardization, also known as ISO, has published information security management system (ISMS) standards that have been recognized and accepted internationally from operational to technical points in assessing high-risk issues (MCMC, 2019). Figure 1 shows the risk assessment guidelines by ISO 27005.

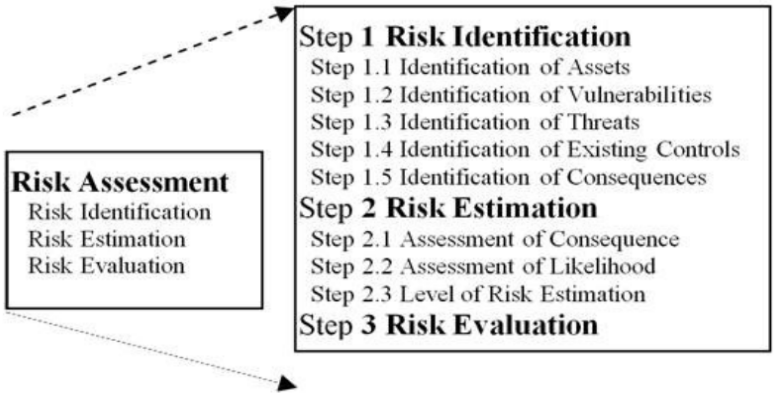

Figure 1. Risk assessment guidelines by ISO 27005 [15]

6.3 Cyber Insurance

According to Thomas Blunck, CEO of Reinsurance Munich Re, quote "Safeguarding our digital world is fundamental to societies and economies. The insurance industry has embraced the pivotal role of cyber insurance in this context since its infancy and even more intensely as the line of business continues to mature. Stakeholders must be prepared for the challenges that the inevitable further intensification of digital dependencies will bring and invest in cyber resilience" unquote (Munich Re, 2023).

6.4 Is Cyber Insurance Truly Necessary?

The greater severity of cyber-attacks has affected companies' transfer risk with cyber insurance. This has resulted in skyrocketing costs of incident response, business disruption, and recovery (Brown, 2022). However, markdown, who has almost 30 years of expertise in cybersecurity, data privacy, and business resilience, insists that most industries have become too digitally dependent on ignoring cybersecurity, which can be a strategic enabler to modern digital business and mitigate financial and operational risks (Brown, 2022).

6.5 Cyber Insurance Risk Management

Cyber risk management is core in a digitised world. Since cyber insurance is an essential part of this, demand continues to grow strongly. Facilitating a sustainable cyber insurance market remains a key task for the insurance industry. Figure 2 shows the global cyber insurance market and its demands (Munich Re, 2023).

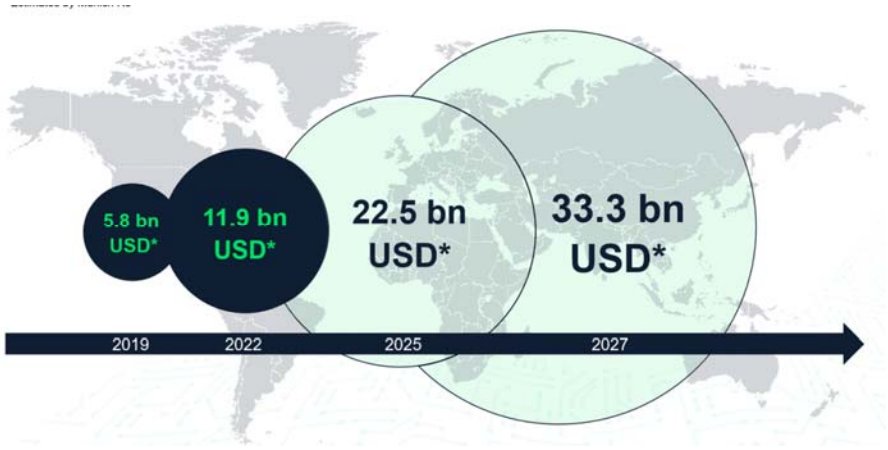

Figure 2. Cyber insurance global market: Demand continues to grow (Munich Re, 2023)

6.6 Cyber Insurance Framework

According to Nor Hasnul et al. in their recent studies, "Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations," the rate of adoption has remained low despite being a target for cyber-attacks in Asia-Pacific (Nur Hasnul et al., 2022).

6.7 Rules and Regulations in Malaysia

In terms of rules and regulations, National Cyber Security Agency (NACSA) has listed Malaysian Cyber Laws on its official portal, which includes the Copyright (Amendment) Act 1997, Computer Crimes Act 1997, Digital Signature Act 1997, Telemedicine Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, Electronic Government Activities Act 2007, Personal Data Protection Act 2010, Penal Code, and Anti-Fake News (Repeal) Act 2020 (NACSA, 2021).

7. Methodology

Figure 3. Research Methodology

Figure 3 shows the Research Methodology used for the research as a whole. As this is an introductory article, the technical framework of the study is not included in this paper.

7.1 Data Collection Sampling

30 semi-structured interviews were conducted in this study to collect the data. The data was collected from 30 experienced Malaysian organizations in the public and private sectors. In the first stage of the semi-structured interview, 25 interviews were carried out. Then, from the interview findings, a focus group session was carried out to validate the results collected in the study's first phase.

Activity:

- Primary and Secondary Data
- Interviews and Questionnaires

Outcomes:

- Interviews data
- Questionnaires data

7.2 Data Analysis

The data collected is used to evaluate and interpret the barriers and enablers contributing to develop the factors influencing the decision to adopt cyber insurance among Malaysian organizations. The collected data be analysed by using a thematic analysis approach. The thematic analysis involves classifying key codes by reading transcripts from in-depth interviews or focus groups to develop themes (Caulfield, 2022).

Thematic analysis is a popular and adaptable qualitative research method that delivers a rich, detailed, yet complex explanation of data (Nowell et al., 2017). Quantitative analysis was implemented to establish the ranking of the most crucial barriers and enablers to cyber insurance adoption by using Kendall's Coefficient of Concordance (W) method. At the same time, the thematic analysis was conducted for qualitative data to create emergent themes from participants' adoption of cyber insurance. The thematic analysis was conducted using NVivo software to code the interview transcripts.

Kendall's Coefficient of Concordance (W) is applied to identify significantly associated groups of the ranking in the barriers and enablers by respondents (Kendall & Gibbons, 1990). Microsoft Excel has been used to calculate the result, along with the formula for Kendall's Coefficient of Concordance (W) based on Kendall and Gibbons (1990) below.

$$W = \frac{(\sum T^2 - \frac{(\sum T)^2}{n})/n}{m^2(n^2-1)/12}$$

The formula is simplified further as follows:

$$W = \frac{12[\sum T^2 - (\sum T)^2/n]}{nm^2(n^2-1)}$$

T = The sum of the ranks for each item being ranked

m = The number of rankings (total number of organizations involved in this research)

n = The number of items being ranked (number of barriers or enablers)

Activity:

- Identify the key factors.

Outcomes:

- The key factors that influence the adoption of cyber insurance.

8. Result and Analysis

8.1 Participated Organisation

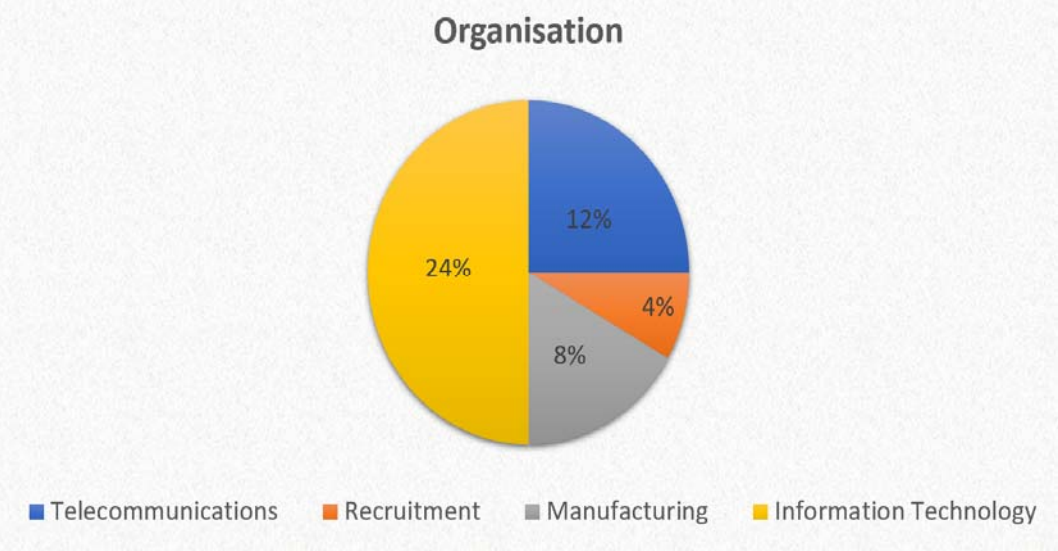

Figure 4. Participated Organisation

As per Figure 4, 24% of participating organisations are from Information Technology, 12% from telecommunications, and 8% from Manufacturing. The least participant is from the Recruitment Industry.

8.2 Years of Experience

Table 1 shows the years of experience of the personnel engaged or participating in the survey.

Table 1. Interviewed personnel years of experience

Industry	1 – 3 years	4 – 6 years	Less than 1 year	More than 6 years	Grand total
Banking	1	1		4	6
Cybersecurity Service			2	5	7
IT		2		4	6
Manufacturing	1	1			2
Recruitment Service				1	1
Telecommunication Service	1	1		1	3
Grand Total	3	5	2	15	25

The most interviewed participants showed that their experience was more than six years in

their field. A small minority of participants (8%) indicated the total experiences that they have had in their area of working for less than a year. Approximately one-third of the participants responded were between one to three years of experience, 12%), and the rest were between four to six years (20%).

9. Conclusion

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 the public and the private sectors, whether for government, business, or Small and Medium Industries (SMEs).

Acknowledgments

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

Abd Rahman, N. H., Raju, R., Ariffin, S., Abdul Hamid, N. H. A., & Ahmad, A. (2022). Adoption of Cyber Insurance in Malaysian Organisations. *International Journal of Innovative Computing*, *12*(2), 45–51. https://doi.org/10.11113/ijic.v12n2.380

Adib, P. (2023). Retrieved June 15, 2023, from https://www.nst.com.my/news/nation/2023/06/920589/new-law-boost-cybersecurity

Alwi, A., & Zainol Ariffin, K. A. (2018). *Information Security Risk Assessment for the Malaysian Aeronautical Information Management System*. https://doi.org/10.1109/CR.2018.8626841

Brown, M. (2022). Do companies need cyber insurance? Retrieved from https://www.techtarget.com/searchsecurity/post/Do-companies-need-cyber-insurance

Caulfield, J. (2022). *How to Do Thematic Analysis | Step-by-Step Guide & Examples*. Retrieved from https://www.scribbr.com/methodology/thematic-analysis

Deloitte Insights. (2020). *A report from the Deloitte Centre for Financial Services Overcoming Challenges to cyber insurance growth*. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/4997_FSI-Cyber-insurance/DI_FSI%20Cyber%20Insurance.pdf

EIOPA. (2019). *Cyber Risk for Insurers – Challenges And Opportunities*. Retrieved from https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf

Fortinet, B. (2023). Retrieved Feb. 22, 2023, from https://www.nst.com.my/news/nation/2023/02/882387/fortinet-malaysia-recorded-84-million-cyber-attacks-daily-fourth-quarter

Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*, *15*(1), 98–114. https://doi.org/10.1111/rego.12266

Internet Security Threat Report (ISTR). (2019). *Symantec Corporation*. Retrieved from https://usa.ingrammicro.com/cms/media/Documents/vendors/s/symantec/istr_24_es.pdf

ISC. (2022). *Cyber Security Workforce Study*. Retrieved from https://www.isc2.org/research

Kendall, M. G., & Gibbons, J. D. (1990). *Rank Correlation Methods*. E. Arnold. Retrieved from https://books.google.com.my/books?id=YFMBwQEACAAJ

Malaysia Communications & Multimédia Commission. (2019). *Technical Code*. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G020_2019-INS-Cyber_Insurance_Acquisition.pdf

Munich, R. (2023). Risk Management Expert Organisation. Retrieved Sept. 12, 2023, from https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html

NACSA. (2021). *Malaysian Cyber Laws*. Retrieved from https://www.nacsa.gov.my/legal.php

Nor Hasnul, A., Normalina, I., Fazlin Marini, H., Rajeswari, R., Humza, N., & Atif, A. (2022). Barriers and enablers to adopting cyber insurance in developing countries: An exploratory study of Malaysian organizations. *Computers & Security*, *122*, 102893. https://doi.org/10.1016/j.cose.2022.102893

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847

OECD iLibrary. (2023). *Organisation for Economic Cooperation and Development* (OECD). Retrieved from https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en

Pavel, T. (2020). *Cyber Insurance Market in Israel – What is the Official Policy*? 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). https://doi.org/10.1109/CyberSA49311.2020.9139722

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

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz002

Skadden. (2023). *SEC Adopts Rules for Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, Skadden, Arps, Slate, Meagher & Flom LLP and*

Affiliates. Retrieved July 27, 2023, from https://www.skadden.com/insights/publications/2023/07/sec-adopts-rules-for-cybersecurity-risk-management

Sohime, F. H., Ramli, R., Rahim, F. A., & Bakar, A. A. (2020). *Exploration Study of Skillsets Needed in Cyber Security Field*. 8th International Conference on Information Technology and Multimedia (ICIMU). https://doi.org/10.1109/ICIMU49871.2020.9243448

Sriram, I., & Mishra, S. (2021). *Understanding risks within Asia Pacific's growing cyber insurance market*. (Verisk Analytics). Retrieved fromhttps://www.verisk.com/insurance/visualize/understanding-riskswithin-asia-pacifics-growing-cyber-insurance-market/

Sunday Daily (Kaspersky). (2023). Retrieved August 9, 2023, from zhttps://www.thesundaily.my/business/malaysia-sees-197-increase-in-web-threats-targeting-businesses-in-2022-according-to-kaspersky-data-DI10905475\

Yan, F. Y. Y., Mohamad, A. M., & Sharon, G. (2022). Regulatory Response to Cybersecurity Risks Management in Malaysia: Case of Worms and Malware. *Research in Management of Technology and Business*, *3*(2), 85. Retrieved from https://publisher.uthm.edu.my/periodicals/index.php/rmtb/article/view/9622

Copyrights