Economic Affairs, Vol. 68, No. 03, pp. 1495-1510, September 2023
DOI: 10.46852/0424-2513.3.2023.17

AESSRA

Review Paper

Impacts of Information Technology and Risk Management on Cybersecurity Governance: Empirical Study on Malaysian Financial Institutions

Suhaily Hasnan[1,2] , Dayana Hamka[3], Alfiatul Rohmah Mohamed Hussain[1], Mazurina Mohd Ali[1], Maslinawati Mohamad[1] and Anderes Gui[4]

[1]Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia
[2]International School, Vietnam National University, Hanoi, Vietnam
[3]Bank Rakyat Malaysia, Kuala Lumpur, Malaysia
[4]School of Information Systems, Bina Nusantara University, Indonesia

*Corresponding author: suhailyhasnan@uitm.edu.my (**ORCID ID:** 0000-0002-6050-8741)

Received: 08-05-2023 **Revised:** 23-07-2023 **Accepted:** 02-08-2023

ABSTRACT

Cybersecurity threats have successfully targeted financial institutions worldwide due to the increased connectivity of seamless and borderless financial services. Considering that criminals have employed more sophisticated methods to exploit the financial industry, financial institutions must adopt an integrated framework to counter the attacks and protect financial infrastructure from exploitation. The study examined cybersecurity governance by extending the Integrated System Theory (IST), including information technology (IT) governance and risk management (RM) governance. Questionnaires were distributed to Malaysian financial institutions through corporate social media platforms, email, and Google Form in November 2021. The questionnaire used a five-point Likert scale and comprised Section A which focused on the respondents' demographic profile, while Section B emphasised the research construction. A total of 128 respondents participated within four weeks. Data obtained from the questionnaire was analysed for descriptive statistics, correlation, and regression analyses. Resultantly, IT governance and RM governance significantly and positively impacted cybersecurity governance. The study provides better insights to the practitioners, academicians, or researchers to identify which factors to be considered and emphasise before developing an integrated cybersecurity governance framework.

HIGHLIGHTS

- This paper is devoted to studying the factors influencing cybersecurity governance by extending the IST.
- In the course of the study, the impacts of information technology governance and risk management governance on cybersecurity governance are explored.

Keywords: Information technology governance, risk management governance, cybersecurity governance, integrated cybersecurity governance framework

The coronavirus disease (COVID-19) pandemic has profoundly impacted the world in numerous ways and government-implemented movement restrictions transformed most physical activities into virtual. Consequently, technology development and advancement are at the greatest speed to accommodate the current demands. Nonetheless, the transformations have caused changes in modus operandi and crime trends. The latest Global Economic Crime and Fraud Survey 2020 issued by

How to cite this article: Hasnan, S., Hamka, D., Mohamed Hussain, A.R., Mohd Ali, M., Mohamad, M. and Gui, A. (2023). Impacts of Information Technology and Risk Management on Cybersecurity Governance: Empirical Study on Malaysian Financial Institutions. *Econ. Aff.*, **68**(03): 1495-1510.

Source of Support: None; **Conflict of Interest:** None

Pricewaterhouse Coopers (PwC) reported cybercrime as the second-highest most disruptive economic crime after customer fraud (PwC International, 2020). In the Malaysian report, cybercrime has increased from 22 per cent in 2018 to 37 per cent in 2020 where the seriousness has doubled from 8 per cent to 16 per cent. Nevertheless, only 45 per cent of the respondents admitted to having a dedicated programme to address cybercrime (PwC Malaysia, 2020). Based on recent police statistics, Malaysia suffered losses of Malaysian Ringgit (MYR) 2.23 billion to 67,552 cybercrime cases between 2017 and June 2021 (New Straits Times, 16 July 2021). The Bukit Aman commercial crime investigation department (CCID) stated that online cheating cases had increased by 60.6 per cent over the last 10 years. Additionally, CCID recorded losses amounting to MYR380 million within the first nine months of 2021 with 15,935 reported cases (Bernama, 27 October 2021).

In another report, PwC 21st CEO Survey 2018 disclosed that cyber threats were ranked as the number one concern of Malaysian bank CEOs where 89 per cent believed that cyber threats negatively impact organisational growth prospects. Moreover, PwC predicted that financial institutions (FIs) are 30 per cent more likely to be targeted by cyber threats than other Malaysian organisations (PwC Malaysia, 2018). Furthermore, over 70 per cent of Malaysian FIs still rely on existing information on technology operations to perform cybersecurity-related functions and responsibilities. In the survey, 58 per cent of board members from Malaysian FIs indicated that reports on cybersecurity matters remain predominantly performed by the Chief Technology Officer as the appropriate designated information security officer. Summarily, the aforementioned report findings suggested that technology is a double-edged sword which develops businesses and empowers individuals who intend to cause harm. Despite the current pandemic situation and the rapid increase of cybercrime cases, a gap exists in enhancing the knowledge of the importance of an appropriate governance framework for cybersecurity.

The high connectedness from the application of borderless information technology (IT) increases the need for a robust cybersecurity governance framework in the FIs, which is more important today than ever. Due to cyber attackers becoming increasingly sophisticated and more persistent, breaches in FIs security defences are no longer a question of ‘if’ but ‘when’. In response to the imminent threat of cyber-attacks, governments and organisations worldwide have regarded cybersecurity as a major priority. The cybersecurity phenomenon extremely affects the developing nations that are transitioning to a digital economy and digital business activity (Antonucci, 2017). The threat of cyber-attacks becomes more significant in the financial sectors where the innovation of new forms of financial services leverages the advancement of internet connectivity. The FIs are exposed to various types of cyber-attacks through the intensive utilisation of IT for core banking systems, internet financial services, digital customer onboarding, and internal communication. The financial industry has been repeatedly targeted with immense success by cyber-attacks.

Severely publicised financial and payment services incidents in the United States (US) included data breaches at JP Morgan, Card Services, Target, and TJX. Verizon reported significant financial markets threats including Distributed Denial of Service (DDoS) attacks, web attacks, cyber espionage, card skimming, and point-of-sale terminal attacks (Catota, 2018). Cyber risks have dramatically evolved and the days of relying solely on the implementation of new security technology as a cyber-defence measure have ended, specifically in the heavily regulated financial sector. McKinsey (2019) mentioned that researchers and regulators continue to emphasise the importance of governance in the implementation of cybersecurity measures to strengthen defence against hackers and intruders regarding transforming cybersecurity.

Cybersecurity involves technology and tools, people, information, systems, processes, and culture. Cybersecurity is about ensuring that technology works, people and processes are aligned with the overall security strategy in the organisation, and every person dealing with the organisation knows how to respond to threats and breaches. Thus, cybersecurity challenges today incorporate issues regarding the people, processes, and the entire issue holistically throughout the FIs. Cyber-attack sophistication and persistence have produced various strategic initiatives for cybersecurity in critical infrastructure protection, including the National Institute of Standards and Technology cybersecurity framework, information sharing programmes, and other cyber strategies (Jaccard & Nepal, 2014).

Cybersecurity research overwhelmingly believes that a holistic approach is essential to counter cyber-attacks instead of solely relying on technical solutions (Al-Darwish & Choe, 2019; Corradini, 2020). Hence, the study considered factors other than technological measures, most importantly, human intervention. Ultimately, the automated security being utilised is managed by humans where any deviation against the pre-set IT security rule may expose FIs to security breaches. The success of such an approach requires a high degree of legal, technological, and economic growth and a competent workforce. Unfortunately, underdeveloped countries frequently lack the capabilities which impair their ability to recognise and respond appropriately to cyber threats. Although cybersecurity risks have significantly evolved over the past few decades, the approaches adopted by FIs are disproportionate to the risks involved. Therefore, the study focuses on IT and risk management (RM) to examine cybersecurity governance.

Regulators and FIs continue to prioritise technological measures in minimising the growing cyber threats. Accenture (2021) reported that organisations worldwide had increased their IT security budgets up to 15 per cent of the total spending in IT itself, which is five per cent higher than IT security spending in 2020. Organisations continuously apply numerous technological strategies to combat cyber-attacks, such as cloud security, network security, virtual private networks, and content filtering (Akhtar *et al.* 2020). Countries are not holding back in placing budgets to ensure cybersecurity is intact. Malaysia allocated MYR1.8 billion to execute the initiatives of the Malaysia Cyber Security Strategy (MCSS) from 2020 to 2024 (The Malaysian Reserve, 13 October 2020). The 2021 budget allocated MYR27 million for Cybersecurity Malaysia to strengthen national cybersecurity, indicating the governmental commitment to combat cybercrime (The Star, 6 November 2020). Cybersecurity in Malaysia offers a diverse range of cybersecurity innovation-driven services, programmes, and projects aimed at reducing the vulnerability of digital systems while bolstering Malaysian cyberspace self-reliance. Nevertheless, given the aggressive increase of cybercrime cases in recent years, the spending of such allocation to mitigate cybersecurity risk remains debatable. Hence, the governance of Malaysian cybersecurity needs to be examined.

The study examined the impact of IT and RM governance on cybersecurity governance. Specifically, the study aims to assess FI participants' level of knowledge and if the particular institutions are implementing various measures (IT governance: security policy, contingency management, and organisational IT goals and RM governance: internal control and risk management) to ensure that key services continue to be provided in the event of a disruption. The situation is accomplished by ensuring that proper precautions are implemented in any unforeseen incidents.

Research focusing on cybersecurity is crucial as FIs need to strengthen vigilance and diligence in the governance aspect and explore new approaches to enhance cyber resilience. The study is useful for academics, professional practitioners, and industrial players that are engaged in the field and to identify effective prevention measures for cybersecurity threats from IT and RM governance perspectives. Additionally, the current findings could assist FIs to assess current capabilities and mechanisms to prevent incidents of cybersecurity threats. The study also provides knowledge and awareness to FIs and practitioners on the benefits of implementing an integrated cybersecurity governance framework of IT and RM and minimising cybersecurity threats.

The study comprises Section 2, which reviews the relevant literature to develop hypotheses on the impact of IT and RM governance on cybersecurity governance. Section 3 presents the research methodology used to conduct empirical research on cybersecurity while Section 4 discusses the results. Lastly, Section 5 concludes the study.

LITERATURE REVIEW

The IT Application in Financial Service Industry

The IT evolution has facilitated daily commercial transactions throughout various financial industries. Financial technology (FinTech) innovation facilitates the development of diverse business models and meets customer demands (Salmony, 2014). FinTech impacts various facets of economics, such as payment services, the banking industry, and financial laws. The term 'FinTech' refers to the growth of IT innovation in the financial service business. FinTech has advanced the development of financial industry applications, processes, products, and business models (Alt & Puschman, 2012). FinTech advancements have created new business models and transformed mechanisms on how individuals interact with financial services, thus attracting the attention of regulators and politicians across jurisdictions. A joint report by the Cambridge Centre for Alternative Finance, Asian Development Bank Institute, and FinTechSpace stated that internet penetration in the Association of Southeast Asian Nations (ASEAN) reached 58 per cent in 2018 and mobile connectivity increased by 141 per cent. Indonesia and Malaysia are among the ASEAN countries with the highest number of FinTech companies with a share of 17 and 11 per cent, respectively. Malaysia has made significant progress as a global FinTech hub in recent years. The FinTech Report 2019 stated that Malaysia has 198 FinTech operating in numerous areas, and FinTech solutions are predicted to grow in the coming years with 95 per cent of Malaysians banked and 86 per cent internet penetration (Diniyya *et al.* 2021). The rising transaction value of internet banking from MYR920.9 million in 2018 to MYR734.9 billion in 2019 demonstrates growth (FinTech Malaysia, 2019).

To support the growth, the FinTech Association of Malaysia was established in 2016 to engage with industry players and support the development of FinTech, and connect with stakeholders locally and globally. Furthermore, Bank Negara Malaysia (BNM) established the Financial Technology Enabler Group (FTEG) in June 2016 to support the development and quality of Malaysian FinTech. The FTEG is a cross-functional group within BNM responsible for developing and improving regulatory policies to aid the adoption of technological innovations in the Malaysian financial service industry.

Cybersecurity in Financial Service Industry

Researchers and academics have proposed numerous interpretations of cybersecurity and the development of IT and the evolution of cyber threats. Craigen *et al.* (2014) mentioned that the definition of cybersecurity differs based on the context, such as sectors, fields, and socioeconomic background. Craigen *et al.* (2014) defined cybersecurity as the *"Organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."*

Meanwhile, Schatz *et al.* (2017) has taken a more inclusive and clear method of defining cybersecurity by considering key components of cybersecurity and global understanding. They proposed the following definition: *"The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace. The concept includes guidelines, policies, and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users."*

Seemma *et al.* (2018) proposed that cybersecurity is the protection of internet-connected systems including hardware, software, and data from cyber-attacks. Cybersecurity includes safeguarding virtual or physical properties against unauthorised access to the data centre and other computerised systems. Therefore, researchers generally agree that cybersecurity is a form of protection of IT against potential threats that can undermine the entire IT system.

In the face of digital disruption, FIs are compelled to follow the FinTech wave by investing heavily in digital transformation to gain a competitive advantage and provide better services. Trust remains a basic underlying value for FIs in providing services mainly to fortify the safety and security of customer assets. Internet as an asset of the electronic environment requires protection from hostile attacks aimed at purposefully damaging FIs (Whitley, 2009; Wang *et al.* 2015).

Currently, cybersecurity is one of the world's most pressing concerns due to being more interconnected than ever. Despite the benefits, increased interconnectedness has resulted in the potential for theft, fraud, and abuse. People worldwide are becoming increasingly reliant on contemporary technology, thus increasing exposure to cyber-attacks, such as corporate security breaches, phishing, blackmail, fraud, and social media fraud (Stevens, 2018). Nonetheless, the security of FIs is presently under severe threat as evidenced by numerous high-profile cases of respected and trusted global and local FIs falling victim to cybercriminals. In August 2014, a US investment bank was targeted in one of the greatest client data breaches in history that resulted in a total estimated loss of MYR4 billion (Mirchandani, 2018). The BNM in 2018 detected and prevented a cybersecurity issue involving illicit financial transfers using forged SWIFT communications. Additionally, the infrastructure of one of the top Malaysian FIs, CIMB, was allegedly infected with ransomware in September 2019 (KPMG Cyber Response, 2018).

The incidents reveal defects in the global financial system as hackers increasingly employ sophisticated tools and strategies to launch assaults. Apart from reputational damage and loss of customers and other key stakeholders' trust, inadequate cybersecurity can impose FIs to fines in certain jurisdictions when personal data security is exploited. The FIs could not afford to overlook cybersecurity given the current situation. A proactive strategy is required to ensure preparedness and resilience. Cybersecurity is changing due to the interconnection of digital ecosystems and their hazards. Therefore, additional resources and investments in cybersecurity are required to bolster FIs security defences.

The IT Governance

The IT governance refers to the structure aligning IT strategy with business strategy which can be appropriately measured if the organisation follows a formal framework. The IT governance in this study consists of three variables: security policy, contingency management, and organisational IT goals.

Implementing a security policy is essential in organisations, specifically when dealing with critical services. A security policy is a detailed description of what is and is not permitted in protecting system security (Bishop, 2003; Stouffer *et al.* 2011). The IST suggested that institutions adopt a formal and documented security policy integrating the following elements: the definition of the policy, the scope of the information security system, RM, the definition of control objectives, and the construction of an applicability statement (Hong *et al.* 2003). Security policies are crucial for ensuring that organisational security practices are adhered to. The study aims to assess participants from various institutions and cross-sectors on their level of knowledge and whether their particular institution is implementing numerous measures to ensure that key services continue to be provided in the case of disruption. The situation is accomplished by ensuring the implementation of proper precautions in the event of any unpredictable incidents. Ismail *et al.* (2016) stated that 57 per cent of the respondents generally agree that the implementation of security policy is essential for risk mitigation of potential threats, aligned with Catota *et al.* (2018) and Alawonde (2020). Nonetheless, Hasan *et al.* (2021) highlighted that several organisations do not adopt adequate security policies despite governmental efforts to enforce the needs.

In contingency management, information security management should be integrated into institutional contingency plans to prevent, detect, and mitigate vulnerabilities and threats to cybersecurity (Ismail *et al.* 2016). Contingency planning encompasses all the activities that institutions are required to perform in ensuring continuous operations in cases of a service outage or a disaster (Carbaugh *et al.* 2019). The planning usually entails paperwork outlining procedures for managing equipment, restoring data, identifying employees' accountability in each activity, and coordinating emergency operations.

Mubarak (2016) mentioned that the activities associated with contingency planning fall under the purview of information security. The contingency aspect equips institutions to respond to situational needs in case of an information security breach. Contingency planning also predicts potential information security issues and advocates planning for an adequate response. Similar to Catota *et al.* (2018), Alawonde (2020) disclosed that most respondents agreed to incorporate a contingency plan across institutions to curb cybersecurity threats.

Based on IST, Ismail *et al.* (2016) measured the extent to which organisations are aware of information security mechanisms and discovered that information security goals are significantly related to the key measurement indicators, such as assessing security policies, RM, internal control, and contingency management. Nevertheless, the current study focuses on examining cybersecurity governance, thus organisational IT goals are regarded as one of the independent variables that positively impact IT governance and subsequently cybersecurity governance. Organisational IT goals refer to the comprehensiveness of necessary elements: processes, people, and technology to address risks arising in the business environment (Alawonde, 2020). Therefore, assessing organisational IT goals aids in measuring IT governance as a whole. Thus, the study hypothesised as follows:

H$_1$: *The implementation of IT governance has a significant positive impact on cybersecurity governance.*

The RM Governance

From the perspective of RM governance, two measurements are included: internal control and RM where internal control states that each organisation should monitor the control performance of its installed security systems (Hong *et al.* 2003). Control is generally defined as the process of preventing, detecting, and correlating system behaviours to prevent unauthorised access and activity in the system (Ismail *et al.* 2016). Stouffer *et al.* (2011) described control as management, operational, and technical control that is integrated into the information system to safeguard the system confidentiality, integrity, and availability. The IST suggests the insufficiency of implementing controls that only minimise threats and vulnerabilities, which must also be audited. Internal control presumes the actions in response to the results of risk analysis and risk assessment (Rahimian *et al.* 2016). Institutions should develop auditing methods to monitor the effectiveness of measures to address information security risks (Casola *et al.* 2019). Control and auditing encompass institutional efforts to prevent, detect, and control information security breaches.

Based on RM, information security threats and vulnerabilities can be recognised, calculated, and assessed through an examination of the risks in an organisation. The hypothesis proposed that the risk assessment outcome could be used to design information security risk control strategies (Ismail *et al.* 2016). The aim of risk management is to implement mechanisms that assist the organisation in reducing risks to an acceptable level (Hong *et al.* 2003). The acceptable risk level varies depending on organisational risk appetite or the quantity and type of risk an organisation is willing to take to accomplish its objectives.

The RM suggests that information security threats and vulnerabilities can be recognised, calculated, and assessed, hence risk assessment outcomes could be used to design information security risk control strategies (Ismail *et al.* 2016). Ismail *et al.* (2016) reported that almost half of respondents agreed on the implementation of a security assessment mechanism, the appointment of a person to perform the assessment, implementation of risk assessment methodology, and awareness programmes to ensure the adequacy of internal control, the findings aligned with Alawonde (2020). Based on the above discussion, the study proposed as follows:

H$_2$: *The implementation of RM governance has a significant positive impact on cybersecurity governance.*

The study also argues that simultaneous integration of IT and RM governance would strengthen the positive impact on cybersecurity governance. Thus, it is hypothesised as follows:

H$_3$: *The integration of IT governance and RM governance has a significant positive impact on cybersecurity governance.*

Integrated System Theory

Hong *et al.*'s (2003) IST for information security management serves as the study theoretical foundation. The overall purpose of IST is to manage information security from the lens of contingency management by integrating security policy, risk management, internal control, and information auditing through the development of organisational information security goals. The five components are based on individual theories which Hong et al. (2003) argued to be inadequate individually.

The IST laid the basis for the research framework on information systems security (Cannoy *et al.* 2006; Järveläinen, 2012), emphasising the critical nature of integrating security components within an organisation to ensure the effectiveness of information security and business continuity in inter-organisational IT relationships. Due to its extensive applicability in other vital sectors, the theory is selected to provide a more comprehensive view of overall security awareness through the application of key measurement indicators. The arising security architecture develops an integrated framework for mitigating information security risks that considers the fast-paced environment where organisations operate today (Alawonde, 2020). Hence, given that the current study focuses on cybersecurity governance, several amendments were made concerning the components to fit the study purpose.

For the conceptual purpose, internal control and information auditing are deemed one variable consistent with Alawonde (2020) and the organisational IT goals variable is added. Moreover, the five variables are categorised into two groups: IT governance and RM governance. Figure 1 illustrates the research framework while the following sub-sections discuss IT and RM governance to posit the study hypotheses.

RESEARCH METHODOLOGY

Sample Selection

The selected study population is based on BNM data, which includes a total of 44 licensed Malaysian FIs comprising Commercial Banks, Islamic Banks, and Development Banks. The unit analysis is compliance officers of the respective FIs. Hirschmann (2021) stated that approximately 376,000 employees were employed under Malaysian FIs in 2020. The samples were selected through convenience sampling which refers to non-probability sampling where a group of individuals of a targeted population meet certain practical criteria conveniently available for the study purpose. Thus, convenience sampling is applicable as its main objective is to gather information from easily accessible respondents.

Roscoe (1975) proposed that a sample size between 30 and 500 is appropriate for most research. Therefore, 250 sets of questionnaires are an appropriate sample for the study. Ismail *et al.*'s (2016) investigation of Supervisory Control and Data Acquisition (SCADA) organisations information security goals randomly selected 118 respondents from employees working in various sectors and received 101 useful responses. Based on the probability in Ismail *et al.* (2016), 300 questionnaires were distributed to ensure the study could obtain 250 responses for relevant analysis. The questionnaires were administered by selecting 10 existing Malaysian FIs. Furthermore, 30 sets of questionnaires were distributed for each of the selected FIs to generate an aggregate amount of 300 sets of questionnaires. Ultimately, the study only received 128 useful responses.

Table 1: Sample Selection

Total population	376,000
Targeted sample	250
Total questionnaires distributed	300
Final useful sample	128

Research Instrument

The survey instrument is the adopted questionnaires from Ismail *et al.* (2016) used to capture respondents' knowledge on whether the institutions they work at are implementing IT governance, RM governance, and cybersecurity governance measures. The survey instrument is subsequently amended and adapted to align with the study objective. The questionnaires comprise 30 items, five items emphasise respondents' demographic profile, and the remaining focus on the variables in IT and RM governance and cybersecurity governance. The questionnaires use a five-point Likert scale comprising (1) strongly disagree, (2) disagree, (3) neutral, (4) agree and (5) strongly agree.

The survey consists of two sections: Sections A and B. Section A entails respondents' demographic profile, such as age, years of experience, education background, the position of employment, and type of FIs. Section B highlights security policy, contingency management, organisational IT goals, internal control, RM, and cybersecurity governance variables, where each variable consists of four measurements. Prior to that, the initial step is obtaining research ethics approval from the university to proceed with distributing the questionnaires to respondents from the targeted population.

Variable Measurement

Table 2 demonstrates the variable measurements for the study.

Table 2: Variable Measurement/Dimensions

Variable	Acronym	Dimensions
Independent Variable: IT Governance		
Security Policy (SP)	SP1	My organisation has a specific and adequate documented IT security policy and procedure.

	SP2	My organisation has adequate internal guidelines in IT hardware or equipment maintenance.
	SP3	My organisation has an adequate policy for portable devices, such as hardware and software.
	SP4	My organisation has documented change management procedures.
Contingency Management (CM)	CM1	My organisation has adequate continuity of operations documentation.
	CM2	My organisation has installed intrusion detection software.
	CM3	My organisation monitors and maintain all logs.
	CM4	My organisation has a designated team to handle disaster recovery from cyber threats.
Organisation IT Goals (IT)	IT1	My organisation implements adequate information technology policies for related systems.
	IT2	My organisation implements adequate security training and awareness programme.
	IT3	My organisation has clear segregation of duties for operating functions related to IT.
	IT4	My organisation provides direct accessibility of well-documented procedures.
Independent Variable: RM Governance		
Internal Control (IC)	IC1	My organisation implements security assessment mechanism.
	IC2	My organisation has appointed person in charge or function to conduct security assessment.
	IC3	My organisation has service acquisition strategy.
	IC4	My organisation manages security training and awareness.
Risk Management (RM)	RM1	My organisation conducts vulnerability assessments.
	RM2	My organisation conducts vulnerability assessments.
	RM3	My organisation existing risk management process help to prevent cyber threats.
	RM4	My organisation manages risk within its risk appetite.
Dependent Variable: CS Governance		
Cybersecurity (CS)	CS1	My organisation has an appointed person in charge to manage security policy and procedure IT.
	CS2	My organisation has adequate disaster recovery documentation.
	CS3	My organisation has procedures in providing adequate training on security architecture and design of related systems.
	CS4	My organisation has specific plans to control and maintain IT security.
	CS5	My organisation has the ability to minimise unfavourable cyber threats.

Data Collection

The questionnaires were prepared, distributed, and collected within one month. Prior to distributing the questionnaires to respondents, the questionnaires were reviewed by five individuals specialising in IT. In order to estimate the response rate and feasibility of the study, a pilot test was conducted where 20 questionnaires were distributed to respondents working in different types of FIs, such as Malaysian commercial banks, Islamic banks, and development banks. The test was important to examine the error of each variable and assist the respondents to gauge their understanding of the survey. The questionnaire distribution was conducted via corporate social media platforms, such as LinkedIn, email, and Google Form. Overall, 300 sets of questionnaires were distributed to selected Malaysian FIs. Before sending the questionnaire through email and Google Form, the respondents were contacted by phone call as a courtesy and requested to further distribute the questionnaires to at least 10 officers in the respective FIs. The questionnaire was distributed on the first week of November 2021, followed by a reminder via phone calls or electronic mail on the second and third week to those who did not respond to the survey. During the fourth week, the data collection was deemed final as no other answered survey was received.

Models

The study used regression models to analyse the relationship between IT governance and RM governance factors and CS governance. All the factors included in the models were selected based on the IST adoption and past findings. The following regression models were utilised to determine the extent of the impact of each factor in the study on CS governance.

$$CS\ Governance = \beta 0 + IT\ Governance\ (\beta_1 SPi(t,1) + \beta 2CMi(t,1) + \beta 3ITi(t,1)) + \varepsilon i\ (t,1) \quad \ldots(1)$$

$$CS\ Governance = \beta 0 + RM\ Governance\ (\beta 4ICi(t,1) + \beta 5RMi(t,1)) + \varepsilon i(t,1) \quad \ldots(2)$$

$$CS\ Governance = \beta 0 + IT\ Governance + RM\ Governance + \varepsilon i(\mathrm{t},1) \quad \ldots(3)$$

RESULTS

Demographic Profile

Table 3 presents the respondents' demographic profiles. For the respondents' age, most were between 26 to 35 years old (45.3%), followed by respondents between 36 to 45 years old (41.4%). Meanwhile, few respondents were below 25 years old (5.5%) and over 46 years old (7.8%). Thus, most respondents were from a matured group of people with cybersecurity exposure in the working environment intensively compared to other groups of age.

Regarding working experience, Table 3 presents the respondent distribution based on their years of working experience in FIs. More than half of the respondents have worked between 11 to 20 years, followed by 43 respondents with six to 10 years of working experience. The remaining have over 20 years (17 respondents) or less than five years (11 respondents) of working experience. Thus, most respondents have working experience between six and 20 years within Malaysian FIs.

Education qualification equips an individual with the competencies necessary for the current study. Table 3 demonstrates that most respondents qualified with the Degree level, which constitutes 78.1 per cent of the total respondents. Meanwhile, 16.4 per cent of the respondents have Masters, followed by 2.3 per cent of Diploma and PhD holders. Only one respondent was in the 'others' group where the respondent obtained Sijil Politeknik. Overall, most respondents have appropriate qualifications from higher learning institutions.

The individual's position in the organisation determines their exposure to the development and implementation of IT governance, RM governance, and cybersecurity governance. From Table 3, most respondents are executive-level which consists of 70 respondents (54.7%), followed by middle management with 45 respondents (35.2%), and top management with nine respondents (7.0%). The least common position is from the support staff group with only four respondents (3.1%). The results indicate that executive and middle levels are usually involved with cybersecurity governance across FIs. The groups of individuals are exposed to IT governance and RM governance in curbing the incident of cybersecurity threats. The results could enhance their knowledge in the area.

Concerning the types of FIs, the highest number of respondents is from commercial banks with 56 respondents (43.8%), followed by Islamic banks with 55 respondents (43.0%), and development banks with 17 respondents (13.3%). Hence, most respondents were from the largest Malaysian banks which impose a higher likelihood of dealing with cybersecurity breaches. Therefore, an integrated cybersecurity framework inclusive of IT governance and RM governance could improvise their existing capabilities in managing cybersecurity threats.

Table 3: Demographic Profile

Variable	Frequency	Percent
Age		
<25 years old	7	5.5
26-35 years old	58	45.3
36-45 years old	53	41.4
>45 years old	10	7.8
Work Experience		
<5 years	11	8.6
6-10 years	43	33.6
ears	57	44.5
>20 years	17	13.3
Education Level		
Diploma	3	2.3

Bachelor's Degree	100	78.1
Master's Degree	21	16.4
Ph.D.	3	2.3
Others	1	0.9
Position in the FIs		
Executive	70	54.7
Support Staff	4	3.1
Middle Management	45	35.2
Top Management	9	7.0
Type of FIs		
Commercial Bank	56	43.7
Development Bank	17	13.3
Islamic Bank	55	43.0

Descriptive Statistics

Table 4 provides the descriptive statistics of all tested variables. Most measurements surpassed 4.00 mean scores. The IT governance comprised three variables: security policy, contingency management, and organisational IT goals. For the security policy variable, the highest mean value was reported for measurements SP3 and SP4, suggesting that the respondents believed that the policy for portable devices, such as hardware and software and change management procedures in FIs are adequate and documented. Regarding the contingency management variable, the highest mean value was scored by CM1, indicating that most respondents believed that organisations have adequate continuity of operations documentation. In terms of organisational IT goals, the respondents believed that the organisation they are working with adopt adequate IT policies for related systems and direct accessibility of well-documented procedures. Nonetheless, CM3 and IT3 concerning monitoring logs and segregation of duties for IT function scored the lowest mean value. The findings suggested that sample firms still lack the mechanisms in the existing firm governance.

The RM governance constitutes two variables: internal control and RM. For the internal control variable, the highest mean value was noted for IC2, suggesting that most respondents agreed that FIs have appointed a person in charge or function to conduct a security assessment. The highest mean value for the RM variable was reported by RM4, signifying that respondents believed that the FIs were able to manage risks within their risk appetite. Nevertheless, the remaining three measurements and two measurements in the internal control variable scored below 4.00, thus proposing that to a certain extent, respondents disagreed that RM governance in the FIs is adequate. Concerning cybersecurity governance, only three measurements surpassed 4.00. Most respondents agreed that the FIs have appointed a person in charge to manage security policy and procedure IT, possess adequate disaster recovery documentation, and formulate specific plans to control and maintain IT security.

The Pearson correlation and Cronbach's alpha were used to determine the variables validity, reliability, and internal consistency. For Pearson correlation, a coefficient value that is significant at 0.05 level or lower indicates that the items are valid and genuine. All measurements in the study were significant at a 0.01 level. For Cronbach's alpha, coefficients should range between 0 and 1 but a score of 0 if all items are absolutely unrelated and approach 1 if all items are completely related. The cut-off value of 0.7 implies an acceptable level of internal consistency. Overall, the total Cronbach's alpha for the study was 0.957, thus indicating a very high level of reliability. Summarily, the questionnaire is valid, reliable, and suitable for further investigation.

Table 4

Panel A: Descriptive Statistics for IT Governance

	Mean	**σ**	**r**	**α**
SP1	4.07	0.604	.516***	0.803
SP2	4.07	0.666	.516***	
SP3	4.09	0.784	.502***	
SP4	4.09	0.782	.443***	
CM1	4.08	0.671	.511***	0.829
CM2	4.03	0.773	.619***	
CM3	3.92	0.809	.382***	
CM4	4.05	0.787	.422***	
IT1	4.13	0.652	.577***	0.821
IT2	4.04	0.767	.571***	
IT3	3.95	0.845	.578***	
IT4	4.13	0.710	.548***	

Panel B: Descriptive Statistics for RM Governance

	Mean	**σ**	**r**	**α**
IC1	4.06	0.649	.511***	0.824
IC2	4.14	0.649	.497***	
IC3	3.96	0.778	.525***	
IC4	3.97	0.709	.520***	

RM1	3.98	0.550	.468***	0.797
RM2	3.85	0.722	.457***	
RM3	3.98	0.699	.506***	
RM4	4.05	0.713	.448***	

Panel C: Descriptive Statistics for CS Governance

	Mean	σ	r	α
CS1	4.15	0.764	.489***	0.790
CS2	4.10	0.697	.544***	
CS3	3.86	0.801	.395***	
CS4	4.15	0.677	.513***	
CS5	3.85	0.722	.457***	

Notes:

*σ: Standard Deviation, r: Pearson's Correlation Coefficient, α: Cronbach's Alpha; SP: Security Policy, CM: Contingency, IT: Information Technology, IC: Internal Control, RM: Risk Management, CS: Cybersecurity; Overall Cronbach's Alpha = 0.957; *** denotes significance at 0.01 level*

Correlation Analysis

Correlation analysis is performed to determine the strength of a connection among the average values of the two variables under study. Table 5 presents the correlation coefficient among the variables. The results suggested that all variables were positively and significantly correlated, where the highest correlation was between IC and CS with a coefficient value of 0.830 at a one per cent level. Meanwhile, the lowest correlation was between CM and RM with a coefficient value of 0.593 at a one per cent level.

The result is not surprising as all the study measurements emphasise governance issues. Pallant (2016) warned that the issue of multicollinearity appears when two or more independent variables are highly correlated at 0.90 or higher. Considering that the correlation coefficient value in the study was below 0.90, multicollinearity is not likely to pose an issue in the regression analysis.

Table 5: Person's Correlation Analysis

(r)	SP	CM	IT	IC	RM	CS
SP	1					
CM	.815	1				
IT	.790	.763	1			
IC	.760	.719	.780	1		
RM	.667	.593	.720	.682	1	
CS	.804	.793	.801	.830	.759	1

Notes:

SP: Security Policy, CM: Contingency, IT: Information Technology, IC: Internal Control, RM: Risk Management, CS: Cybersecurity; All Person's correlation coefficient (r) are significance at 0.01 level; n=128.

Multicollinearity Test

In order to prove that multicollinearity was not an issue, the study also performed a multicollinearity test. Numerous difficulties may arise in the regression model due to the presence of multicollinearity within the set of independent variables. Hence, multicollinearity is determined before performing the regression analysis. Multicollinearity can be detected using the tolerance and variance inflation factors (VIF) to assess whether a collection of multiple regression variables exhibits multicollinearity. Hair et al. (2014) described that tolerance denotes the degree of variability in the chosen independent variables that are unaccounted for by other variables, whereas VIF is the inverse of the tolerance value.

The tolerance value of 0.10 is the industry standard cut off limit for VIF values below 10, which means that multicollinearity occurs when the tolerance value is under 0.10 and the VIF value is larger than 10. In the collinearity analysis in Table 6, Panel A presents the findings for the IT governance factor, followed by Panel B for the RM governance factor, and Panel C for both. The results indicated no multicollinearity between the variables. Based on the results, the current study did not encounter any multicollinearity issues because all the variables exhibited tolerance exceeding 0.1 and a VIF value of less than 10.

Table 6

Panel A: Collinerity Statistics for IT Governance

	Collinearity Statistics	
	Tolerance	VIF
SP	0.268	3.733
CM	0.298	3.352
IT	0.333	3.000

Panel B: Collinerity Statistics for RM Governance

	Collinearity Statistics	
	Tolerance	VIF
IC	0.535	1.869
RM	0.535	1.869

Panel C: Collinerity Statistics for CS Governance

	Collinearity Statistics	
	Tolerance	**VIF**
IT Governance	0.309	3.241
RM Governance	0.309	3.241

Notes:

SP: Security Policy, CM: Contingency, IT: Information Technology, IC: Internal Control, RM: Risk Management, CS: Cybersecurity; n=128.

One-Way Analysis of Variance (ANOVA)

Apart from the multicollinearity test, ANOVA was performed to determine the model relevance in predicting cybersecurity governance. The ANOVA of variables in the IT governance is depicted in Table 7: Panel A, followed by RM governance in Panel B, and both factors in Panel C. Overall, the ANOVA test yielded significant results for all three models, thus suggesting that at least one of the factors had a significant linear relationship with cybersecurity governance. Therefore, a significant difference exists between at least one of the independent variables and the dependent variable.

Table 7

Panel A: One-Way ANOVA for IT Governance

	SS	**df**	**MS**	**F**	**Sig.**
Regression	27.626	3	9.209	120.0	0.000
Residual	9.513	125	0.077		
Total	37.139	128			

Panel B: One-Way ANOVA for RM Governance

	SS	**df**	**MS**	**F**	**Sig.**
Regression	28.169	2	14.084	196.3	0.000
Residual	8.970	126	0.072		
Total	37.139	128			

Panel C: One-Way ANOVA for CS Governance

	SS	**df**	**MS**	**F**	**Sig.**
Regression	30.323	2	15.162	278.1	0.000
Residual	6.815	126	0.055		
Total	37.139	128			

Note: *SS: Sum of Squares, df: degrees of freedom, MS: Mean Square, F: F value, Sig.: p-value.*

Regression Analysis

Table 8 presents the multiple regression results for IT governance, RM governance, and the overall CS governance in Panel A, B, and C, respectively. The IT governance results revealed that all the measurements had a significant linear relationship with CS governance. Firstly, the result disclosed a significant positive relationship between security policy and CS governance ($\beta = 0.280$, $t = 3.336$, $p \leq 0.01$), hence implying that the availability of security policy in IT governance positively impacted the success of CS governance.

Secondly, the results suggested a significant positive relationship between contingency management and CS governance ($\beta = 0.250$, $t = 3.440$, $p \leq 0.01$), thus proposing that FIs are expected to implement continuity of documentation, disaster recovery, installation of intrusion data software, and maintain all the logs to enhance CS governance. Thirdly, the findings noted a significant positive relationship between organisational IT goals and CS governance ($\beta = 0.315$, $t = 4.462$, $p \leq 0.01$); thus, H1 is supported. The results aligned with Ismail et al. (2016) where security policy has the highest t-value, which constitutes a higher path of significance towards organisational information security goals. Alawonde (2020) added that security policy is useful to identify foreseeable risks during the risk assessment process to formulate the process. Nevertheless, organisational IT goals in the study depicted the highest t-value, indicating that organisational IT goals are a significant variable that should be included in IT governance.

From the perspective of RM governance, the results indicated a significant positive relationship between internal control and CS governance ($\beta = 0.558$, $t = 9.719$, $p \leq 0.01$). Therefore, most FIs realise the importance of implementing an internal security assessment mechanism by appointing a person in charge to perform relevant assessments and audits to form a service acquisition strategy. The results demonstrated a significant positive relationship between risk management and CS governance ($\beta = 0.363$, $t = 6.003$, $p \leq 0.01$) consistent with Ismail *et al.* (2016) and Alawonde (2020).

Ismail *et al.* (2016) highlighted that RM constitutes the lowest t-value, thus implying that their sample organisation still used default platform configurations due to the system complexity. In the current study, RM scored the second-highest after internal control among other variables. Alawonde (2020) stressed that respondents agreed and confirmed that RM is crucial to deploy strategies in mitigating information security risks. The occurrence of massive corporate scandals created awareness for organisations to focus more on the RM process to prevent cyber-attacks and other frauds instead of fixing the situation after the damage has been done.

The results revealed that IT governance (β = 0.457, t = 6.622, $p \leq 0.01$) and RM governance (β = 0.487, t = 7.066, $p \leq 0.01$) were positively and significantly associated with CS governance. Referring to the multiple R, R-square and adjusted R-square values in Table 8, the highest score was CS governance including IT and RM governance. Hence, IT and RM governance significantly and positively impacted the realisation of CS governance. Therefore, hypothesis H3 is supported.

In Table 2, all the questions are queried around the relationship between independent variables and CS governance. Specifically, the study hypothesis assessed whether the independent variables positively impacted the dependent variable. The findings implied that the overall regression model was significant. Thus, indicating the likelihood to incorporate IT governance and RM governance into an integrated cybersecurity governance framework. Given that the current study examined the cybersecurity governance in Malaysian FIs, the findings could be utilised specifically in financial services in line with the study objective.

Table 8

Panel A: Multiple Regression Analysis for IT Governance

	USC		**SC**	**t**	**Sig.**
	β	ε	**β**		
C	0.597	0.184		3.246	0.002
SP	0.280	0.084	0.293	3.336	0.001
CM	0.250	0.073	0.286	3.440	0.001
IT	0.315	0.071	0.351	4.462	0.000
R	0.862				
R^2	0.744				
Adj.R^2	0.738				
ε	0.277				

Panel B: Multiple Regression Analysis for RM Governance

	US		**S**	**t**	**Sig.**
	β	ε	**β**		
C	0.328	0.190		1.731	0.086
IC	0.559	0.058	0.584	9.719	0.000
RM	0.363	0.060	0.361	6.003	0.000
R	0.871				
R^2	0.758				
Adj.R^2	0.755				
ε	0.268				

Panel C: Multiple Regression Analysis for CS Governance

	US		**S**	**t**	**Sig.**
	β	ε	**β**		
C	0.125	0.168		0.748	0.456
IT	0.149	0.023	0.457	6.622	0.000
RM	0.261	0.037	0.487	7.066	0.000
R	0.906				
R^2	0.820				
Adj.R^2	0.813				
ε	0.234				

Notes:

USC: Unstandardised Coefficients, SC: Standardised Coefficient, β: Beta value, **ε***: Standard Error, t: t-value, Sig.: p-value.*

SP: Security Policy, CM: Contingency, IT: Information Technology, IC: Internal Control, RM: Risk Management, CS: Cybersecurity.

The multiple regression equation as follows:

Cybersecurity Governance = 0.125 + 0.149 (IT Governance) – 0.261 (RM Governance) + ε

From the perspective of IT governance, all the measurements suggested a positive and significant linear relationship with CS governance. Regarding security policy, the findings aligned with Ismail *et al.* (2016) and Alawonde (2020), which suggested that most security breaches are influenced by the security policy. Security policy is useful for identifying potential risks during the risk assessment process, which will then formulate the RM framework (Alawonde, 2020; Saleemi, 2022). Ismail *et al.* (2016) noted the highest t-test value for security policy compared to other tested variables, which indicates that most organisations have implemented adequate security procedures. Additionally, Ismail *et al.* (2016) suggested that most respondents (57%) agreed that security policy implementation is essential to minimise any unwanted risks.

Based on the IST, institutions are required to adopt a formal and documented security policy to ensure the significance of IT governance across institutions (Hong *et al.* 2003). The findings on contingency management also aligned with Ismail *et al.* (2016) and Alawonde (2020), hence indicating that FIs are expected to implement continuity of documentation, disaster recovery, installation of intrusion data software, and maintenance of all the logs. Mubarak (2016) stated that contingency management facilitates predicting potential incidents of cybersecurity threats by advocating planning in response to the threats. Meanwhile, the t-test value reported the highest score for organisational IT goals compared to other factors in IT governance, thus indicating that incorporating organisational IT goals in the IT governance is appropriate to improve the overall cybersecurity governance.

The two measurements of RM governance outlined a positive and significant relationship with CS governance. The findings are supported by Ismail *et al.* (2016) and Alawonde (2020), where both studies discovered that internal control has a significant positive relationship with organisational security objectives. Ismail *et al.* (2016) outlined the implementation of security mechanisms, the appointment of a person in charge of security assessments, service acquisition strategy, and management of security training.

Nevertheless, they documented that internal control had the lowest t-value than other variables and they believed the increment of technology-specific knowledge for practitioners involved with the SCADA system minimises the possibility of future system attacks due to default platform configurations. The RM findings are supported by Ismail *et al.* (2016) where several participating organisations still use the default platform configurations due to the complexity of the systems configurations.

The participants in Alawonde (2020) agreed and confirmed that RM is crucial to deploy strategies in mitigating information security risks. Ismail *et al.* (2016) stressed the significance of organisational financial capability in procuring security measures and equipped personnel with adequate proper knowledge of the system. Based on the IST, the internal audit function and RM are essential in minimising identified threats and vulnerabilities by monitoring the effectiveness of controls adopted across institutions (Rahimian *et al.* 2016).

CONCLUSION

The implementation of cybersecurity governance is vital due to the wider evolution of technology in this era. Therefore, adopting an integrated cybersecurity governance framework inclusive of IT governance and RM governance has become essential to mitigate the risk of cyber-attack occurrences. Generally, although FIs have implemented cybersecurity governance, the execution of an integrated cybersecurity governance framework could strengthen existing capabilities in managing the occurrence of cybersecurity threats. An integrated cybersecurity governance framework is one of the tools that could facilitate the FIs to manage and mitigate cybersecurity threats which may lead to organisational reputational risks.

The study provides better insight to practitioners, academicians, and researchers. The findings enable practitioners, specifically the top management in IT and RM departments can identify the necessary factors before formulating a cybersecurity governance framework to mitigate the risk of cybersecurity breaches. Moreover, employees with IT and RM background may opt to have a wider view than traditional practices by adopting an integrated cybersecurity governance framework.

Due to the pandemic outbreak, practitioners must equip stronger defence against cyber threats to safeguard from reputational risk due to security breaches. Institutions may stay competitive in the market by having concrete defence through an integrated governance framework. Theoretically, the study adopted and adapted the IST popularised by Hong *et al.* (2003). The current study focused on cybersecurity governance, the elements considered as contingency management to achieve organisational objectives in Hong *et al.* (2003) were combined and categorised into two main factors, namely, IT governance and RM governance to formulate an integrated cybersecurity governance framework (see Figure 1). The framework can be applied as guidance by FIs and non-FIs to develop cybersecurity governance that best suit the organisation.

Although the evolution of cybersecurity exploitation is rapidly growing in Malaysia, not many FIs have adopted an integrated cybersecurity governance framework to minimise such incidence. The study only provides a cursory examination of the overall adoption factors, thus future researchers should improve the model employed in the study by adding or removing a construct. Further research on the topic is strongly advised. The pandemic has evolved the working from home concept, increasing exposure to cybersecurity breaches worldwide. The current study proposed that additional research should widen the sample coverage, extend the time frame, and conduct an in-depth analysis of cybersecurity risks in various types of FIs or non-FIs using qualitative methods. Conclusively, the study is beneficial to provide practitioners and academicians with a better understanding and insight into an integrated cybersecurity governance framework and their assimilation in Malaysia.

ACKNOWLEDGMENTS

The Authors would like to express their gratitude to the Research Management Centre, Universiti Teknologi MARA for funding the research project through the Geran Penyelidikan Khas (600-RMC/GPK 5/3 (078/2020)) and the Faculty of Accountancy, Universiti Teknologi MARA for facilitating this research project

REFERENCES

Accenture. 2021. How Aligning Security and the Business Creates Cyber Resilience. Retrieved from https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Akhtar, S., Sheorey, P.A., Bhattacharya, S. and Ajith Kumar, V.V. 2020. Cyber Security Solutions for Businesses in Financial Services. *Int. J. Business Intelligence Research,* **12**(1): 82-97.

Alawonde, K. 2020. Tailored Information Security Strategies for Financial Services Companies in Nigeria. Walden Dissertations and Doctoral Studies.

Alt, R. and Puschmann, T. 2012. The Rise of Customer-Oriented Banking - Electronic Markets are Paving the Way for Change in The Financial Industry. *Electronic Markets,* **22**(4): 203-215.

Al-Darwish, A.I. and Choe, P. 2019. A Framework of Information Security Integrated with Human Factors. In International Conference on Human-Computer Interaction, 217-229. Springer, Cham.

Antonucci, D. 2017. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Audible Studios.

Bernama. 2021. 15,935 Online Fraud Cases, RM380mil in Losses in First 9 Months of 2021. Retrieved from https://www.freemalaysiatoday.com/category/nation/2021/10/27/15935-online-fraud-cases-rm380mil-in-losses-in-first-9-months-of-2021/

Bishop, M. 2003. What is Computer Security? *IEEE Security and Privacy Magazine,* **1**: 67-69.

Carbaugh, E., Antonio, C., Lynch, T. and Nelsen, L. 2019. A Contingency Plan for Catastrophic Loss of Bioassay Services. *Health Physics,* **116**(1): 105-108.

Cannoy, S., Palvia, P.C. and Schilhavy, R. 2006. A Research Framework for Information Systems Security. *J. Information Privacy and Security,* **2**(2): 3-24.

Casola, V., de Benedictis, A., Riccio, A., Rivera, D., Mallouli, W., and de Oca, E.M. 2019. A security monitoring system for internet of things. *Internet of Things,* **7**: 100080.

Catota, F.E., Morgan, M.G. and Sicker, D.C. 2018. Cybersecurity Incident Response Capabilities in the Ecuadorian Financial Sector. *J. Cybersecurity,* **4**(1).

Corradini, I. 2020. Redefining the Approach to Cybersecurity. *Studies in Systems, Decision and Control,* pp. 49–62. https://doi.org/10.1007/978-3-030-43999-6_3

Craigen, D., Diakun-Thibault, N. and Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review,* **4**(10): 13-21.

Diniyya, A.A., Aulia, M. and Wahyudi, R. 2021. Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study. *J. Islamic Economics, Finance, and Banking,* **3**(2): 67.

FinTech Malaysia. 2019. Malaysia FinTech Report 2019. Retrieved from https://fintechnews.my/wp-content/uploads/2019/12/Touch-n-Go-eWallet-Malaysia-Fintech-Report-2019.pdf

Hair Jr, J.F., Sarstedt, M., Hopkins, L. and Kuppelwieser, V.G. 2014. Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool in Business Research. European Business Review.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *J. Information Security and Applications,* **58**: 102726.

Hong, K., Chi, Y., Chao, L.R. and Tang, J. 2003. An Integrated System Theory of Information Security Management. *Information Management and Computer Security,* **11**(5): 243-248.

Ismail, S., Sitnikova, E. and Slay, J. 2016. SCADA Systems Cyber Security for Critical Infrastructures. *Int. J. Cyber Warfare and Terrorism,* **6**(3): 79-95.

Jaccard, J.J. and Nepal, S. 2014. A Survey of Emerging Threats in Cybersecurity. *J. Computer and System Sciences,* **80**(5): 973-993.

Järveläinen, J. 2012. Information Security and Business Continuity Management in Inter-Organizational IT Relationships. *Information Management and Computer Security,* **20**: 332-349.

KMPG Cyber Response. 2018. Clarity on Cyber Security. KPMG. Retrieved from https://assets.kpmg/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf

McKinsey. 2019. Perspectives on Transforming Cybersecurity. Digital McKinsey and Global Risk Practice. Retrieved from https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

Mirchandani, B. 2018. Laughing All the Way to the Bank: Cybercriminals Targeting U.S. Financial Institutions. Forbes.

Mubarak, S. 2016. Developing a Theory-Based Information Security Management Framework for Human Service Organizations. *J. Information, Communication and Ethics in Society,* **14**(3): 254-271.

New Straits Times – Basyir, M. 2021. Malaysia Suffered RM2.23 Billion Losses from Cyber-Crime Frauds. Retrieved from https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds

Pallant, J. 2016. SPSS Survival Manual (6th Ed.). McGrawHill Education.

PwC International. 2020. PwC's Global Economic Crime and Fraud Survey 2020. Retrieved from https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2020.pdf

PwC Malaysia. 2020. PwC's Global Economic Crime and Fraud Survey 2020 – Malaysia Report: Fraud and Corruption - Malaysia has its Say. Retrieved from https://www.pwc.com/my/en/assets/publications/2020/PwC-Global-Economic-Crime-and-Fraud-Survey-2020-Malaysia-report.pdf

PwC Malaysia. 2018. 21st CEO Survey the Anxious Optimist in the Corner Office. Retrieved from https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf

Rahimian, F., Bajaj, A. and Bradley, W. 2016. Estimation of Deficiency Risk and Prioritization of Information Security Controls: A Data-Centric Approach. *Int. J. Accounting Information Systems,* **20**: 38-64.

Roscoe, J.T. 1975. Fundamental Research Statistics for the Behavioural Sciences, 2nd Edition. New York: Holt Rinehart & Winston.

Salmony, M. 2014. Access to Accounts: Why Banks Should Embrace an Open Future. *J. Payments Strategy and Systems,* **8**(2): 157-171.

Schatz, D., Bashroush, R. and Wall, J. 2017. Towards a More Representative Definition of Cyber Security. *The J. Digital Forensics, Security and Law.* https://doi.org/10.15394/jdfsl.2017.1476

Saleemi, J. 2022. Crypto Market and Liquidity Risk in Environments due to Pandemic Uncertainty. *J. Contemporary Research in Business, Economics and Finance,* **3**(4): 168–178.

Seemma, P.S., Nandhini, S. and Sowmiya, M. 2018. Overview of Cyber Security. Int. J. *Adv. Res. in Computer and Communication Engineering,* **7**(11): 125-128.

Stevens, T. 2018. Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance,* **6**(2): 1-4.

Stouffer, K., Falco, J. and Scarfone, K. 2011. Guide to Industrial Control Systems (ICS) Security. Office of the Press Secretary.

The Malaysian Reserve – Yunus, R. 2020. Malaysia Introduces New Cyber Security Strategy. Retrieved from https://themalaysianreserve.com/2020/10/13/malaysia-introduces-new-cyber-security-strategy/

The Star – Yeoh, A. 2020. Budget 2021: RM27mil Allocation for CyberSecurity Malaysia Hailed by Industry Players. Retrieved from https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players

Wang, B., Zheng, Y., Lou, W. and Hou, Y.T. 2015. DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking. *Computer Networks,* **81**: 308-319.

Whitley, E.A. 2009. Informational Privacy, Consent and the "Control" of Personal Data. *Information Security Technical Report,* **14**(3): 154-159.