Research in Management of Technology and Business Vol. 3 No. 2 (2022) 085–097
© Universiti Tun Hussein Onn Malaysia Publisher's Office

RMTB

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/rmtb
e-ISSN : 2773-5044

Regulatory Response to Cybersecurity Risks Management in Malaysia: Case of Worms and Malware

Felicia Yong Yan Yan[1], Ani Munirah Mohamad[2,*] & Grace Sharon[3]

[1] Lee Kong Chian Faculty of Engineering and Science, Department of Surveying, Universiti Tunku Abdul Rahman, 53300 Kuala Lumpur, MALAYSIA

[2] School of Law and Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia, 06010 Sintok, Kedah, MALAYSIA

[3] Faculty of Law, Universitas Krisnadwipayana, Jawa Barat 13077 Jakarta, INDONESIA

*Corresponding Author

DOI: https://doi.org/10.30880/rmtb.2022.03.02.008
Received 30 September 2022; Accepted 01 November 2022; Available online 01 December 2022

Abstract: The increase in use of information and communication technologies (ICTs) brings about risks and ramifications, one of which is the intrusion of worms and malware into the computer systems and networks. Accordingly, a strong regulatory response needs to be in place to protect the users of the ICTs to avoid any unwanted incidents to the individual, the organisation as well as the nation. This study aims at highlighting case analysis of worms and malware attacks involving five (5) selected case studies, and the regulatory response to the cyber risks management in Malaysia, focusing on worms and malware attacks. Engaging in socio-legal approach, involving two datasets of worm and malware incidents, and written legal rules, the analysis was carried out using content and doctrinal analyses. The study reported five (5) selected case study incidents and three (3) pieces of written rules on the regulation of worms and malwares, being the Computer Crimes Act 1997, Guidelines on Management of Cyber Risks (2016) and Risk Management in Technology (2020). In addition, few international standards are also discussed. The implication of the study is better appreciation of the worm and malware incidents in the global context, as well as regulator's initiatives in addressing such incidents in Malaysia. This paper could become a catalyst in studies of regulatory response mechanisms within the context of cybersecurity and cybersecurity risks management.

Keywords: Cyber risks, Cybersecurity, Cyber crimes, Risk management, Regulatory response

Corresponding author: animunirah@uum.edu.my
2022 UTHM Publisher. All rights reserved.

1. Introduction

Worms and malware are among the greatest hazards to computer systems and networks. A malicious piece of software that replicates itself and transmits itself to other computers is known as a computer worm. It regularly spreads via computer networks, and in order to get access to the machine it targets, it looks for vulnerabilities in the system's security. This computer will act as a host for the purpose of scanning and infecting other personal computers. In most cases, the damage that worms do to their host networks is caused by the use of bandwidth and the overloading of web servers. It's possible for worms to carry "payloads" that cause harm to the host computers they infect. Payloads are pieces of malware that are meant to carry out operations on infected workstations in addition to spreading the worm itself. These activities may include sending spam or installing further malware.

Malware (short for "malicious software"), on the other hand, is a file or code, supplied via a network, that infects, examines, steals, or does any action an attacker desires. Malware may, in short, wreak havoc on a computer and network. Hackers use it to discover passwords, delete data, and render computers worthless in their quest for information. A malware attack can cause chaos on the organization's regular operations and long-term protection.

Few studies have pointed out the risks and dangers of worms and malware in computer systems and networks, detections and risks management, such as the ones by Qasem and Al-Saedi (2017), Rozenberg, Gudes and Elovici (2008) and Yamaguchi (2020). Nevertheless, literature has highlighted the need for more case studies on worms and malware to better comprehend the risks management strategies for addressing the risks involved in this situation (Broucek and Turner, 2013; Rahman, 2012; Rahman, 2017; Nelson, 1990). Given the vast potential for breaches and ramifications of worms and malware to the organisation, it is therefore pertinent that regulations be put in place to develop viable cyber risks management strategies to be adopted by organisations. Unfortunately, within the context of Malaysia, very few literatures have reported on the regulatory response to cyber risks management particularly for cases on worms and malware in organisations.

Therefore, to achieve the research objectives incidents of worms and malware attacks involving five selected case studies are analysed. Consequently, the regulatory response to the cyber risks management in Malaysia, focusing on worms and malware attacks is examined.

The following sections deliberate on the review of literature on the major themes used in the study, the methodology undertaken, followed by the findings of the study.

2. Literature Review

This section provides an account of the key themes engaged in this study, being cybersecurity risks, cybersecurity risks management, as well as worms and malware.

2.1 Cybersecurity Risks

The advancement of technology is constantly taking astonishing and sometimes unsettling new forms. Today, personal relationships, work schedules, and commercial decisions not only rely on technical tools, but individuals frequently rely on them. This opens a door of opportunity for enterprising computer hackers. Accessibility to vast quantities of sensitive information exposes an increasing number of firms to a variety of cyber dangers, from data theft and ransomware to corporate espionage – and they may not even realise it (Garfinkel 2012; King *et al.*, 2018). Although "cyber risk" may be understood literally, however the technical definition might carry different meanings to different people. it is not always well-defined and might have different connotations to different individuals. Cyber risk is, however, the danger of damage to an organisation resulting from its information technology (Alahmari and Duncan, 2020).

Another term that was coined in this context is known as cybersecurity risk, and it refers to the possibility that the company could suffer exposure or loss as a result of a cyber attack or data breach. With the increased digitalization of company information and documents, such companies are more susceptible to worms and malware attacks. Data breaches, a widespread form of cyber attack, frequently result from inadequate data protection and have devastating effects on businesses (Boletsis *et al.*, 2021). (Boletsis *et al.*, 2021). The danger of cyber attacks from both inside and outside the firm is rising because of worldwide connection and the increasing usage of cloud services with poor security vulnerabilities. What information technology (IT) risk management and access control could solve in the past must now be supplemented with sophisticated cyber security people, software, and cybersecurity risk management.

2.2 Cybersecurity Risks Management

In the present world of cybersecurity risk management, one uncomfortable truth is evident: enterprise-wide cyber risk management is more difficult than ever before. Keeping architecture and systems secure and compliant can be daunting for even the most talented teams of today (Lee, 2021). A growing number of laws and regulations control how personal data must be protected within organisations (Jarjoui and Murimi, 2021). Today's businesses are held liable for data processing performed by third parties on their behalf. As if managing our own risk was not difficult enough, modern enterprises must now manage vendor risk.

Managing the risks caused by poor cybersecurity safeguards is an integral aspect of any business operations. The danger landscape is constantly in flux. The discovery of new exploits is followed by the release of patches to remedy them. Frequently, new potentially vulnerable devices are added to the network, which increases the attack surface (Kejwang, 2022). This is especially true considering the rapid expansion of Internet of Things (IoT) devices and sensors being installed in several physical locations. Cybersecurity risk management must be ongoing if defences are to be maintained. Existing cybersecurity risk planning is also impacted by variables besides the ever-changing nature of threats. Frequently, regulations are revised, or new ones are enacted. The associated risks must be examined, and cybersecurity policies and procedures must be modified to assure compliance.

The rapid pace of technological advancement makes the management of cybersecurity risks an absolute necessity for modern businesses. Both small and large enterprises must recognise that the present cyber dangers can make the organisation an attractive target for an attacker. Even the largest corporation with the most customers is susceptible to attack (Moturi, Abdulrahim and Orwa, 2021). (Moturi, Abdulrahim and Orwa, 2021). A cyberattack on an organisation that is not prepared could result in the loss of data, as well as negative impacts on the company's finances, brand reputation, and employee morale (Kejwang, 2022).

Organizations must create and implement a risk management strategy to remove cyber-attack threats and mitigate business-specific hazards. A cyber risk management strategy can assist decision-makers in understanding the risks associated with daily operations (Lee, 2021). A cyber risk assessment will assist the organisation in determining the potential of cyber-related assaults to which it is susceptible (Perols and Murthy, 2021). A cyber risk management strategy can assist a corporation in identifying the most significant threats, enabling it to allocate resources and time effectively. This will also aid in the prevention of the hazards identified during the assessment.

2.3 Worms and Malware

The essential function of a computer worm is to duplicate itself and infect other computers while remaining active on infected systems. (Feng 2022). Hackers frequently send phishing emails or instant messages with malicious attachments to spread computer worms for the first time. The goal of cybercriminals is to mask the worm so that the target will run the programme. Double file extensions and/or data names that seem innocent or urgent, such as "invoice," are used to achieve this goal. When

the user downloads the attachment or link, the malware (computer worm) will be downloaded into the system or they will be redirected to a malicious website (Achar, Baishya and Kaabar, 2022). The worm gains access to the user's system in this way without their knowledge. Once run, the worm attempts to grow and enter more systems. For instance, the worm may send an email containing copies of itself to all contacts on the infected machine.

On the other hand, malware is an umbrella name for viruses, worms, trojans, and other hazardous computer software that hackers employ to create havoc and access sensitive data. It refers to any programme that is aimed to do harm to a single computer, server, or computer network (Pinhero, *et al.*, 2021). In other words, rather than a specific method or technology used in its development, malicious software is recognised based on its intended use (Chinebu, Udegbe and Eberendu, 2021). Typically, cybercriminals utilise it to extract or encrypt data that they may exploit for financial benefit through ransom demands (Eze and Chukwunonso, 2018; Sethia and Jeyasekar, 2019). The types of information that can be compromised have expanded to include everything from financial information to medical records to personal emails and passwords (Ray and Mohanty, 2021). Although malware cannot harm the actual hardware of systems or network equipment (with one known exception), it may steal, encrypt, or wipe your data, modify or hijack vital computer functions, and surreptitiously monitor a user's computer activity.

3. Research Methodology

This section outlines the methodology undertaken in the study, including the research design, data collection process and the data analysis.

3.1 Research Design

The study adopted the socio-legal approach, combined with case studies of selected cases on worms and malware within organisations. The social aspect of the study involved the review of literature and selected actual cases of detected worms and malware within organisations. This approach is necessary to address the first objective of the study. Meanwhile, for the second objective of the study, a doctrinal legal approach was engaged, particularly in determining the statutory and regulatory aspects of cyber risks management strategies within organisations focusing on worms and malware cases.

3.2 Data Collection

Two types of data were collected for the purpose of the study; firstly, case study data involving five (5) selected worms and malware incidents reported in the global context, and secondly, legal rules on cyber risks management of worms and malware within organisations.

The case study data was extracted from public domain or search engines using the keywords of ‘computer worm’, ‘computer malware’, ‘worm and malware’, ‘cyber risks of worms and malware’ and few other related keywords. The inclusion criteria included year of incidents to be in the past 20 years i.e., in between 2002 and 2022, complete information on reporting agency, damage caused to the organisation and punishment of the offender. This data is pertinent to address the first objective.

Meanwhile, for the legal rules, data sources include statutory provisions, rules and regulations within the Malaysian context providing for cyber risks and cyber risks management, and worms and malware particularly. This data is pertinent to address the second objective.

3.3 Data Analysis

The data collected in the study was analysed using content and doctrinal analysis for the purpose of highlighting the incidents of worms and malware attacks, as well as presenting the regulatory response to the cyber risks management in Malaysia.

4. Results and Discussion

This section deliberates on the findings of the study after the analysis, presented based on the two objectives of the study, i.e., case analysis of worms and malware attacks involving five (5) selected case studies, and the regulatory response to the cyber risks management in Malaysia, focusing on worms and malware attacks.

4.1 Case Analysis of Worms and Malware Attacks

For this study, with respect to the first objective on analysis of incidents of worms and malware attacks, five (5) case studies for the past 20 years were analysed. The background of the attacks, the damage caused as well as the sanctions accorded to the perpetrators were highlighted. Also, from the five (5) case studies, worms are found to be more prevalent as opposed to malware.

(a) Case 1 – Year 2003: the Sobig Worm

In August 2003, the Sobig Worm (computer worm) tainted millions of Internet-connected Microsoft Windows systems internationally, including Canada, the United Kingdom, the United States, continental Europe, and Asia, exacerbating world's total losses amounting to $30 billion. Sobig is the second quickest computer worm to have gone wild since Mydoom. Despite several remarks indicating that worm experiments might be tracked back to August 2022, multiple Sobig worm versions were published immediately. The first instance of Sobig.A was found in January 2003. Sobig.B, originally known as Palyh, was launched on May 18, 2003. On May 31, 2003, Sobig.C, which fixed the timing issue in Sobig.B, was released. Sobig.D was found a few weeks later, followed by Sobig.E. On June 25, 2003. Sobig.F was discovered and establish a fastest time metastasizing email worm on August 19, 2003. The Sobig.F variety is the most widespread and devastating.

Experts from the University of California and other institutions discovered that the worm could infect more than 75,000 computers in a mere 10 minutes, doubling the number of affected machines every 8.5 seconds. These led Microsoft to offer $250,000 from their $5 million Anti-Virus Reward Programme in exchange for information to apprehend and convict the worm's developer. Some worm experts refer to similarities between the worm and Send-Safe, a spamming programme written by Ruslan Ibragimov, a native of Moscow, Russia, as a suggestion that Ibragimov and potentially a team of developers had developed the worm. Ibragimov refuted such a notion by pointing out its shortcomings. Furthermore, he indicated that he had lost many clients since the advent of the Sobig worm. Although Sobig's developer is still unknown, nevertheless, four distinct characteristics that must be understood in identifying the Sobig worm's developer are: (1) expert knowledge of the worm; (2) development ability; (3) Souce code access; and (4) Motivation to develop such malware.

(b) Case 2 – Year 2004: Mydoom

my.doom, W32.MyDoom@mm, Novarg, Mimail.R and Shimgapi are also known as Mydoom, a computer worm encountered on January 26, 2004, and disrupted Microsoft Windows. It broke the record for the most widespread email worm set by the Sobig worm and ILOVEYOU. As of 2022, this record has yet to be shaken. The initial emails sent to Russian ISPs were traced by Kaspersky Labs' location-sensing software, which allowed the country of origin of Mydoom to be determined. The outbreak was linked to Russian networks and exhibits all the traits of worms created by Russian phishing scams and crime syndicates: it instals an open mediator that spammers use to send spam email and a backdoor that lets thieves set up key loggers and other tools to steal credit card numbers, passwords, and other sensitive data.

Mydoom consists of a few variants, notably Mydoom.A and Mydoom.B. Mydoom has tainted over 50 million devices worldwide. One out of every 41 emails and as many as one out of 12 emails at once were infected by Mydoom.A. Shortly after being released into the public, it accounts for 20–30% of all

email traffic worldwide, slowing down internet traffic all around the world. The harm inflicted by Mydoom and its derivatives cost $52.2 billion (inflation-adjusted sum) despite a projected value of $38.5 billion back in 2004. It would cost four or five times as much because of the extra time and resources necessary to defend the systems. Hence, the SCO Group, who holds the Unix rights, offered a $250,000 reward for information leading to the capture and conviction of the Mydoom.A worm author, while Microsoft provided a similar incentive towards the Mydoom.B worm creator targeting their website. Despite this, nobody knows who invented Mydoom. Besides that, the SCO Group also sued many Linux manufacturers and supporters, alleging that part of its proprietary code was utilised in the system. SCO sued Novell (previous proprietors of SuSE, now a part of Attachmate), AutoZone, and Daimler-Chrysler and was sued by Red Hat and IBM. Such conduct sparked widespread outrage in the open-source community, as many think they were implicated. Many open-source organisations worldwide refuted this and decried the development of viruses and worms.

(c) Case 3 – Year 2008: Conficker

Conficker, also known as Downup, Downadup, and Kido was discovered in November 2008. This computer worm attacks the Microsoft Windows operating system. It spreads by exploiting flaws in Windows OS software and weak passwords on administrator passcodes to create a rootkit, and it has been substantiated to be pretty difficult to combat due to its use of many sophisticated and improved malware tactics. When Conficker infects a computer, it immediately disables a number of different security measures and automated backup settings, deletes restore points, and enables connections to a remote machine in order to receive instructions from that machine. By setting up the first machine, Conficker might exploit and get access to the remainder of the network. Millions of computer systems from government, business, and families in over 190 countries were infected by Conflicker worm, making it the biggest computer worm infestation since the 2003 Welchia.

On February 12, 2009, Microsoft made an announcement regarding the formation of an industry group that would be referred to as the Conficker Cabal in an effort to combat Conficker. They reported their findings in the Journal of Sensitive Cyber Research and Engineering, a secret, peer-reviewed United States government cybersecurity magazine. It was determined that a gang of con artists operating in Ukraine were the ones responsible for creating this malware. According to the findings of Porras and colleagues, the criminals gave up on Conficker after it had progressed farther than they had anticipated. They claimed that any effort to exploit it would draw an excessive amount of attention from law authorities throughout the world. In the field of cybersecurity, this line of thinking is largely accepted. In 2011, Ukrainian police detained three Ukrainians in relation with Conficker following close coordination with the Federal Bureau of Investigation (FBI) (FBI) (FBI). Despite this, there is no evidence that they were ever brought to trial or convicted of any crime. After acknowledging his guilt, the Swedish national Mikael Sallnert was given a prison term of forty-eight48 months in the United States of America.

(d) Case 4 – Year 2010: Stuxnet

Stuxnet is thought to have been in existence since 2005 but only found in 2010. It is a vicious computer worm to have exacerbated major harm to Iran's nuclear programme by artistically attacking distributed control systems. Stuxnet is claimed to have influenced numerous centrifuges at Iran's Natanz uranium enrichment site to burn out. According to other organisations that have updated this material, the worm's ultimate goal is to destroy critical infrastructure, such as water treatment facilities, power plants, and piping. These targets will be identified in the future. In contrast to other forms of malware, Stuxnet does relatively less harm to machines and networks that do not meet the exact setup requirements that it specifies. The attackers "took precautions to ensure that only their picked targets were struck. It was a marksman's job," according to Ralph Langer, an independent computer security expert. Such complexities are uncommon in malware. Even though the worm is not selective, if Siemens software is not found on computers that have been infected, the worm enters a dormant state and

contains protections that prevent it from spreading to more than three additional devices on each infected workstation before it destroys itself on June 24, 2012. Stuxnet contains the source code necessary to carry out a man-in-the-middle attack. This exploit pretends to be sensor signals used in industrial process control in order to stop an infected machine from shutting down as a consequence of anomalous behaviour.

The worm is thought to be a malicious payload that was jointly created by the spy agencies of the United States and Israel as part of Operation Olympic Games. Neither country has explicitly acknowledged active participation in the operation, but the widespread belief is that both countries were involved. Further investigation by Wikileaks led to the discovery of a diplomatic document in which the United States was given the recommendation to target Iran's nuclear capabilities through the use of "covert sabotage." This recommendation was originally made by the Bush administration, but it was pushed forward by the Obama administration. Yossi Melman, who wrote a book about Israeli intelligence and covered intelligence for the Israeli newspaper Haaretz, was another person who suspected Israeli involvement. Melman also wrote a book about Israeli intelligence. Israel has been suspected of being the nation that is responsible for Stuxnet through the use of Unit 8200, according to reports from the media as well as experts such as Richard A. Falkenrath, who previously worked as the former Senior Director for Policy and Plans within the United States Office of Homeland Security.

(e) Case 5 – Year 2014: Heartbleed

The OpenSSL cryptographic library, as a result of the Transport Layer Security (TLS) protocol, included a flaw known as Heartbleed. It was published through software in 2012 and released publicly in April 2014. The vulnerable OpenSSL instance, regardless of wether functioning as a TLS server or client, could be exploited by Heartbleed. It was caused by improper authentication mechanism (owing to a lacking bounds inspection) in the TLS heartbeat enhanced version implementation. This may be where the glitch probably originated from - heartbeat. The problem was classed as a buffer over-read, which happens when more data is read than should be authorised. Ostensibly, Heartbeat extension secures the SSL and TLS standards by validating server requests. However, Heartbleed weakens the Heartbeat extension, which undermines the security of SSL and TLS server and client communication. Consequently, Heartbleed program enables anyone with internet connectivity to read the memory of systems encrypted by vulnerable versions of the OpenSSL software.

According to the developer who discovered the "Heartbleed" vulnerability in the open-source code used by thousands of websites, it was a "oversight," but the discovery of the flaw verifies the reliability of the methods used. In 2011, Robin Seggelmann, a German computer programmer, supplied code for an upgrade that facilitated the Heartbeart operate in OpenSSL towards secure channels. However, an omission in the upgrade resulted in a serious consequence with the unintended introduction of Heartbleed vulnerability. Seggelmann started working on the OpenSSL project from 2008 to 2012 during his Phd work but is no longer affiliated with it. He further informed the Guardian that "I am willing to take responsibility for the error," he continued, "because I authored the script and overlooked the requisite verification by a monitoring. Regrettably, this blunder also slipped through the evaluation process and hence made its way into the released version." Millions of personal computers and billions of smartphones have been compromised. The bug allows an attacker to force the server to hand out information from its memory that should not be accessible. According to a Netcraft survey conducted in 2014, 17 percent of SSL servers (about 500,000 servers) were susceptible to *Heartbleed*.

4.2 Regulatory Response to Cybersecurity Risks Management

With respect to the second objective of the study, i.e., the regulatory response to the cybersecurity risks management in Malaysia, focusing on worms and malware attacks, there are three major written rules which are highlighted, being Computer Crimes Act 1997 (Act 563), Securities Commission's Guidelines on Management of Cyber Risks (issued in 2016) and Central Bank of Malaysia's Risk Management in Technology (2020). Additionally, various international standards are also found to be related to cyber risks management and presented in this section.

(a) Computer crimes act 1997 (Act 563)

The Computer Crimes Act 1997 provides for computer-related offences and to supplement existing criminal laws. This Act came into force on June 1, 2000 and contains various computer offences It does not define "*hacking*" or "*computer crimes*" specifically, rather the term used is "*unauthorised access to computer material*". Hence, issues such as unauthorised access to computer material, unauthorised access with the aim of committing other crimes, and unauthorised alteration of computer data, and the like are addressed as per Sections 3, 4 and 5 respectively under the Act. It also includes provisions to facilitate investigations for the purpose of enforcing the Act.

Particularly for the case of worms and malware attacks, the relevant section would be Section 5 of the Act that provides that a person might be found liable if he knowingly causes an unauthorised alteration of the contents of a computer or system. Accordingly, with the release of worms or malware into the computer system or network without the authorisation of the owner of the computer system or network, knowingly that the release would cause modification or change to the other party's computer system or network, for instance deleting files, cloaking folders, modifying the contents of the system, or transmitting data packets back to the perpetrator, this would entail the fulfillment of the requirements under Section 5 of the Act. The operational mechanism of unauthorised modification vide Section 5 of the Act is described in Figure 1.

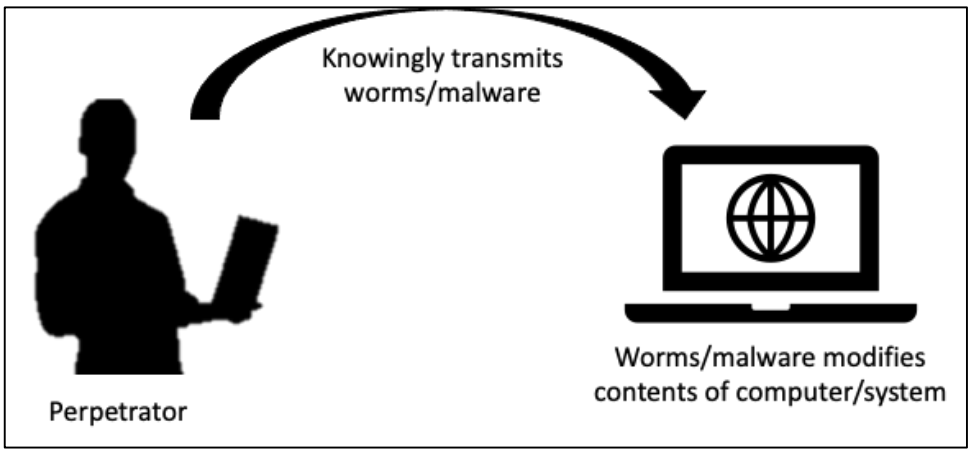

Figure 1. Operational mechanism of unauthorised modification

If someone commits the offence of unauthorized modification vide this Section, he faces potential fine of RM100,000 or jail term of seven years, or if it involves intention or knowledge to cause hurt, the fine could be RM150,000 or 10 years jail term.

(b) Securities commission's guidelines on management of cyber risks (2016)

The Securities Commission (SC) of Malaysia issued the Guidelines on Management of Cyber Risks on 31 October 2016, following the Capital Market and Services Act 2007. The Guidelines apply to all capital market entities in Malaysia. It stipulates the tasks and functions of the directors and top managers of the company on the handling of cyber risk, the development and implementation of cyber risk processes and regulations by capital market entities, and the specifications for handling cyber risk and reporting to the SC.

The introductory provision of the Guidelines defines certain key concepts relevant to the management of cyber risks, such as cyber incidents, cyber risk, cyber threat and cyber resilience. In essence, the Guidelines promote the cyber resilience of capital market entities particularly to put in place proper risk management strategies for cyber threats. In a world where business entities are connected to one another for a plethora of arrangements, connectivity using the Internet is inevitable. Hence, given that the Internet is a double-edged sword, in both providing valuable opportunities as well as risks, it only makes sense that proper risk management strategies should be the priority for businesses.

In this regard, the SC has taken a highly proactive action in introducing this Guidelines, which contains two major parts, firstly, on the governance of cyber risks particularly on the tasks entrusted to the directors and top managers, and secondly on the management of cyber risks itself. Such management strategies comprise implementing cyber risk policies and processes, cyber risk measures such as reporting lines, prevention methods, detection and recovery from cyber risk incidents. The key aspects of the Guidelines are shown in **Figure 2**.

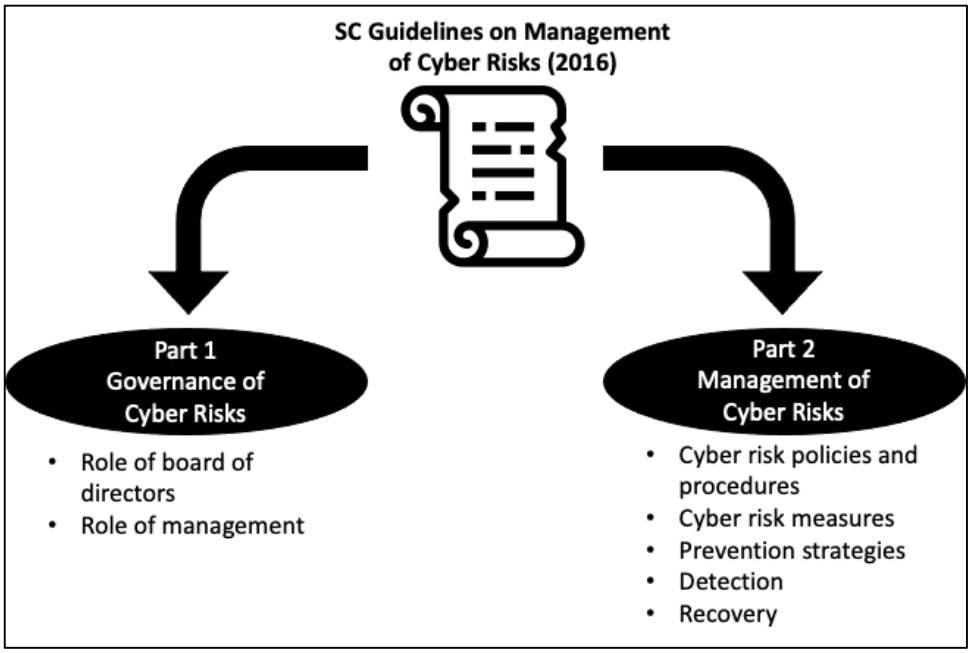

Figure 2. Key aspects of SC guidelines on management of cyber risks (2016)

(c) Central bank of Malaysia's risk management in technology (2020)

Central Bank of Malaysia (CBM) issued the Risk Management in Technology (RMiT) on 19 June 2020 in accordance with Section 266 of the Financial Services Act 2013, Section 277 of the Islamic Financial Services Act 2013 and Section 126 of the Development Financial Institutions Act 2022. RMiT applies to licensed financial institutions including licensed banks, approved issuers of electronic money,

operators of designated payments systems and other licensed financial institutions. It delineates the requirements pertaining to the financial institutions' risk management while using IT systems, applications, platforms and infrastructures.

Financial institutions should be well aware of the scale and complexity of their operation in complying with the requirements. As such, larger and more sophisticated financial institutions should put in place a more rigorous risk management practices, policies and processes that are in line with their growing exposure of technological risks. The policy requirements provided in RMiT is produced in the following **Figure 3**.

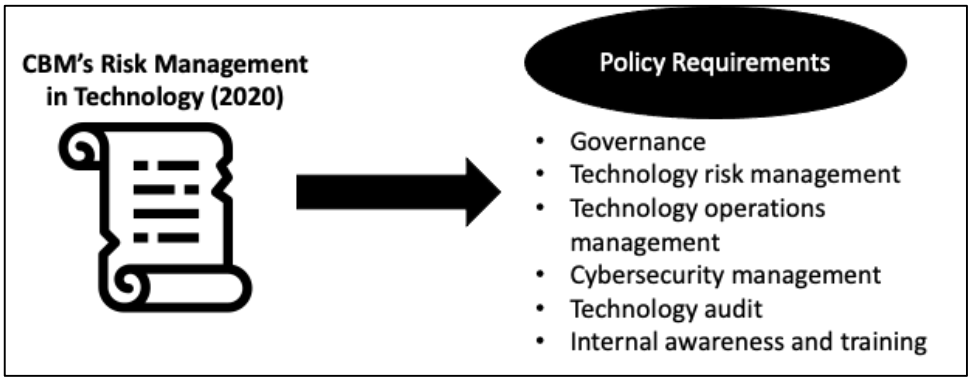

Figure 3. Policy requirements provided in RMiT

(d) Various international standards

A number of international standards are found to provide guidelines on cybersecurity risks management within organisations. For the purpose of this study, four (4) standards are deliberated i,e. International Standard Office's ISO/IEC 15408: 2022 and ISO/ IEC 27005: 2018, as well as National Institute of Standards and Technology, US Department of Commerce's NIST SP 800-30 and NIST SP 800-39, as presented in the following **Table 1**.

Table 1: International Standards on Cybersecurity Risks Management

Item	Scope/Aim	Aspect for Cybersecurity Risks Management
ISO/IEC 15408: 2022	Information security, cybersecurity and privacy protection	Conceptual aspects of various potential cyber attacks and protection against information privacy
ISO/ IEC 27005: 2018	IT security techniques	Risk on security of information
NIST SP 800-30	Risk assessments	Strategies on how to manage cyber risks
NIST SP 800-39	Information security risks	Strategies on how to manage cyber risks within the organization (more detailed)

As shown in Table 1, there are several international standards documents on cybersecurity risks management. However, given the nature of standards, they are persuasive in nature and do not hold a binding effect. In addition, non-compliance of the standard requirements does not come with sanctions. Nevertheless, compliance with such standards would provide recognition to the organisations in terms

of standing and public recognition of the practicability and conformity to the accepted norms of the industry.

5. Conclusion

The study sought to achieve two objectives, i.e. to provide case analysis of worms and malware attacks involving five (5) selected case studies, and analyse the regulatory response to the cyber risks management in Malaysia, focusing on worms and malware attacks. The first part of paper provided an account of the key concepts engaged in the study, being cybersecurity risks, cybersecurity risks management, as well as worms and malware. While, the second part of this paper presents the findings of the study based on the predetermined objectives.

The completion of the research allowed for the extraction of two key results from the overall data collected. The first focuses on the five (5) case studies on worms and malware attack episodes that meet the inclusion criteria laid forth in the methodology section of this article. These case studies were selected because they fulfilled the inclusion criteria. It was discovered that perpetrators of cybersecurity crimes used a variety of methods to release worms and malware into the computer systems or networks of their victims, regardless of whether the victims were using their computers for personal or organisational purposes. The victims and the relevant organisations who had their computer data or system hacked have essentially sustained a significant amount of harm as a direct consequence, which has resulted in both financial and emotional pain.

The second major finding of the study is the account of various regulatory responses to the cybersecurity risks management focusing on worms and malware attacks. First, the study deliberated on the Computer Crimes Act 1997, particularly on Section 5 of the Act which provides for unauthorised modifications to the contents of the computer system or network. In this regard, the government has shown due emphasis on cybersecurity risks entailing the crimes of release of worms and malware with the knowledge that such release would cause harm or damage to the victim. The other two Guidelines were issued by two major regulators in Malaysia covering securities and banking sector, i.e. the SC's Guidelines on Management of Cyber Risks (2016) and CBM's Risk Management in Technology (2020). Both the Guidelines provide two primary regulatory requirements, i.e. on the governance of cyber risks, and the management of such risks. Finally, the study also deliberated on the international standards issued by the International Standard Office as well as the National Institute of Standards and Technology, US Department of Commerce. Essentially, these standards are highly pertinent in setting out standard requirements for organisations to put in place certain procedures and policies within the organisation to manage cyber risks accordingly.

What could be gathered from the findings of the study is the proactive role of the regulators in introducing laws, guidelines and standards for the governance and management of cybersecurity risks within organisations in Malaysia. It seeks to address a whole range of cyber concerns with the emergence of the digital era. Needless to say, incidents of worms and malware attacks would very well be understood to fall within the ambit of the regulatory requirements as reported in the findings of the study. Nevertheless, having such regulations in place could be well supplemented by voluntary creation of internal policies of the respective organisations, so that the management and employees would be guided by their own internal policies which could be modified based on the industrial needs of the organisations.

Accordingly, future research should be directed towards investigating the impacts of these regulations on actual case studies of worms and malware attack incidents. Therefore, it is suggested that future research be carried out empirically in the form of impact study to address the application of the regulations as being practiced and enforced within organisations, as well as the internal policies of the organisations to supplement the regulatory requirements.

Acknowledgement

The authors would also like to thank School of Law and Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia.

References

Achar, S. J., Baishya, C., & Kaabar, M. K. (2022). Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives. Mathematical Methods in the Applied Sciences, 45(8), 4278-4294.

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE.

Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., & Surridge, M. (2021, February). Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In VISIGRAPP (3: IVAPP) (pp. 266-274).

Broucek, V., & Turner, P. (2013). Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective. Journal of Computer Virology and Hacking Techniques, 9(1), 27-33.

Çayır, A., Ünal, U., & Dağ, H. (2021). Random CapsNet forest model for imbalanced malware type classification task. Computers & Security, 102, 102133.

Chinebu, T. I., Udegbe, I. V., & Eberendu, A. C. (2021). Epidemic Model and Mathematical Study of Impact of Vaccination for the Control of Malware in Computer Network. Journal of Advances in Mathematics and Computer Science, 36(3), 72-96.

Feng, C. (2022, August). Discussion on the Ways of Constructing Computer Network Security in Colleges: Considering Complex Worm Networks. In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1650-1653). IEEE.

Garfinkel, S. L. (2012). The cybersecurity risk. Communications of the ACM, 55(6), 29-32.

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In Advances in cybersecurity management (pp. 139-161). Springer, Cham.

Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. International Journal of Research in Business and Social Science (2147-4478), 11(6), 334-340.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9, 39.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.

Moturi, C. A., Abdulrahim, N. R., & Orwa, D. O. (2021). Towards adequate cybersecurity risk management in SMEs. International Journal of Business Continuity and Risk Management, 11(4), 343-366.

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. International Journal of Financial Engineering, 8(02), 2150019.

Nelson, B. (1990). Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm, 11 Computer LJ 299 (1991). UIC John Marshall Journal of Information Technology & Privacy Law, 11(2), 6.

Perols, R. R., & Murthy, U. S. (2021). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. Auditing: A Journal of Practice & Theory, 40(1), 73-89.

Pinhero, A., Anupama, M. L., Vinod, P., Visaggio, C. A., Aneesh, N., Abhijith, S., & AnanthaKrishnan, S. (2021). Malware detection employed by visualization and deep neural network. Computers & Security, 105, 102247.

Qasim, O., & Al-Saedi, K. (2017). Malware Detection using Data Mining Naïve Bayesian Classification Technique with Worm Dataset. Int. J. Adv. Res. Comput. Commun. Eng, 6(11), 211-213.

Rahman, R. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. Computer Law & Security Review, 28(4), 403-415.

Rahman, R. (2017). The Need for More Legal Materials for Better Understanding of Malware and Badware Threats in Malaysia. Mediterranean Journal of Social Sciences, 8(1), 134.

Ray, M., & Mohanty, B. K. (2021). Fuzzy Dynamic Model for the Malware Attack and its Defence in Computer Network. Journal of Optoelectronics Laser, 40(12), 123-131.

Rozenberg, B., Gudes, E., & Elovici, Y. (2008, December). A distributed framework for the detection of new worm-related malware. In European Conference on Intelligence and Security Informatics (pp. 179-190). Springer, Berlin, Heidelberg.

Sethia, V. and Jeyasekar, A. (2019). Malware Capturing and Analysis using Dionaea Honeypot. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-4). IEEE.

Yamaguchi, S. (2020). White-hat worm to fight malware and its evaluation by agent-oriented Petri nets. Sensors, 20(2), 556.