Review on the Enhancement of Cyber Security Policies That Impacts the Employment System

Geevitha Batumalai
School of Computing
Universiti Utara Malaysia
Kedah, Malaysia
geevitha@soc.uum.edu.my

Mohamad Fadli Zolkipli
School of Computing
Universitu Utara Malaysia
Kedah, Malaysia
m.fadli.zolkipli@uum.edu.my

***Abstract*— In today's environment that almost everything has been digitalized, cyber security policies are crucial because of various security concerns and cyber-attacks. Security issues frequently affect many new developments. Security concerns prevent emerging technologies from being adopted and used, even if they have the potential to completely transform systems and people's lives. The constant improvement of cyber security policies has benefited both companies and employees. The research reviews enhancement of cyber security policies affects the employment system, notwithstanding the sacred importance of cyber security policies in the digitalized world. The review show that cyber security policies are essential for secure applications and a safer workplace. Although the idea of cyber risks conjures up images of outsiders, like hackers, attacking a company's systems or carrying out data theft, the most significant vulnerability in workplaces is typically the individuals who work there, which is the employees. This study concludes a better grasp of how cyber security policies affect the employment system.**

Keywords—cyber security policies, employment system, technology

I. INTRODUCTION

Although the growth of information and communication technology, such as the expanded availability of internet access, has profited everyone including organizations, but still cyber security policies are the one that adding the core value in working environments. We might assume that no one else can see or use our personal information for their own purposes. Manufacturers, however, are responsible for making sure our digital products are as safe as possible. To be in the safe side, therefore the organizations provide their own laptops to the employees so that the confidential information of the company will be kept secured within the level of their observation and the maintenance of their property is well managed and professionally standardized.

The frequency of cyber-attacks is gradually rising as information technology advances. Therefore, organizations are expecting a positive return on their investment as they devote significant resources to addressing the issue of workplace cyber hazards and grow more concerned about it (Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar & Xiaohong Yuan, 2019). Furthermore, employees may track problems related to cyber security that have been emerging on a real - time basis, therefore, they must practice judgment over the sorts of countermeasures to be taken when encountered any kind of cyber-attacks. As cyber-attacks are encountered from the technology, the technology itself will aid in overcome these cyber-attacks which we could say technology helps technology. For instance, the blockchain technology. Munir Abu Bakar and Sherin Kunhibava (2018), stated that to utilizing the efficiency advantages that blockchain technology offers, using it could be the solution to Malaysia's cyber security issues and a way to lessen the susceptibility of both public and commercial companies in Malaysia to cyber-attacks.

Cyber security often related to organizational prospects in most context. Peer behavior, cues to action, and employee experience all make up the employee's workplace environment. Employees themselves are playing the significant role in practicing cyber security in workplace. Almost all places have their policies regarding the cyber security. As conventional Work From Home (WFH) transitioned to Work From Office (WFO) due to the pandemic crisis, organizations tend to advocate for tighter cyber security in the workplace. This research would like to review the cyber security enhancement and its impacts on employment system as the cyber security policies are keep evolving as the technology advances.

In next part, this article will cover the literature review followed by the cyber security and policies, cyber security policies which affects the employment system following by threats and cyber security challenges which finally continue with the conclusion on how enhancement of the cyber security in the employment system will ensure the integrity and professionalism in working environment.

II. LITERATURE REVIEW

Defending systems, networks, and software against online threats is the process of cyber security, according to Cisco. These breaches frequently try to hinder typical business activities, steal money from clients via ransomware, or get access to, modify, or delete crucial data or information. There have been several cyber security issues. These problems draw our attention away from the growing importance of protecting the organization's ICT infrastructure. If businesses wish to protect their clients' data from online hackers and dangerous software, they must take cyber security into account. Kamil Tarhan (2022), stated that these policies seek to establish the region as a hub for communications and multimedia, increase access to local information resources and cultural representation, foster consumer confidence in the sector, ensure equitable utilization of infrastructure services, and, most importantly, guarantee information security, network dependability, and integrity Communications and Multimedia Act 1998. Evidently, national security is not the only priority regarding cyber security.

In fact, there is a vast potential of referent objects in the field of cyber security, ranging from persons, organizations, and organizations of every type, national governments, even global networks of both state actors and the non-state actors (Bunoit Dupont & Chad Whelan, 2021). Some physical cyber securities of industrials are wireless sensor networks (WSNs) which is a collection of autonomous or self-processing sensors that are spatially distributed and operate together to accomplish many activities, including monitoring, detecting, and recording, make up WSNs (Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, & Charith Perera, 2022). Other technologies that being implemented in physical to avoid cyber security threats are like Internet of Things for Industry. The phrase Internet of Things (IoT) is a technology which emerged from ICS, such as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) which include networked devices, networking structures, and services. Sensors, controllers are some other examples to protect industrial systems and infrastructure (Fazlan Abdullah, Nadia Salwa Mohamad, & Zahri Yunos, 2018).

III. RESULTS AND DISCUSSION

Data protection, data retention, and access control, as well as website security, cloud computing security which includes email security, physical and network security, information security and privacy were shown to be shared traits among five different business types. The most crucial element to safeguard sensitive data was discovered to be the privacy policy. Some CS policies were shown to be more important than others (Alok Mishra, Yehia Ibrahim Alzoubi, Asif Qumer Gill & Memoona Javeria Anwar, 2022).

A. Policies on cyber security

The increase of cybercrime in Malaysia may be impacted by the lack of filtering or control of Internet policies (Nawi et al., 2022). The Malaysian government has long recognized the necessity for raising public awareness of and comprehension of cyber security-related issues as well as for fostering a culture that values cyber security. Therefore, the government will emphasize the need for self-control on the part of people, groups, or parents (Nawi et al., 2022). Power also strengthens a person or institution. In general, the distribution of a nation's laws will give an individual or organization more influence. Therefore, in order for the body cyber security implementers to play a larger role and act comprehensively in controlling cyber security, power is also a very important requirement.

National Cyber Security Policy (NCSP) which adopted by the Ministry of Science, Technology and Innovation (MOSTI), which will play a role as a roadmap for addressing Malaysia's cyber security issues. This country's national cyber security strategy seeks to help Malaysia move toward a knowledge-based economy where it is also called K-economy. The National Cyber Security Framework provided the foundation for the policy, which covers institutional, international, public-private, technological, legal, and regulatory components (A. Reeves, P. Delfabbro, & D. Calic, 2021). The policy also addressed the Vital National Information Infrastructure (CNII), which it consists of the major industries' networked information systems. (Hamzah, Ahmad, Hussin, & Ibrahim, 2018). For education itself, there are currently two policies in Malaysia that deal with the deployment of e-learning which is Dasar e-Pembelajaran 1.0 and Dasar e-Pembelajaran 2.0. Unfortunately, neither policy has carefully examined how secure each domain is according to the National e-Learning Policy (Alya Geogiana Buja, Noor Afni Deraman, Siti Daleela Mohd Wahid & Mohd Ali Mohd, 2021).

The Malaysian Communications and Multimedia Commission is responsible for enforcing the Communications and Multimedia Act 1998. Sections 211 and 233, out of a total of 282 sections, are those that deal with cyber security. Additionally, the outcomes of the document analysis revealed that Section 233 defines offences related to the abuse of network resources (Nawi et al., 2022). It is important to focus on and consider how elements including parental upbringing, peer pressure, professional roles, the role of the media, and government legislation might assist internet users in defending themselves against cyber dangers. Additionally, a major factor in preventing or lessening cybercrime is the application of cyber legislation. Stricter penalties and the requirements of cyber legislation can help Malaysia's cybercrime problem.

B. Impacts of cyber security policies

Such security measures include, for instance, security policies that safeguard an organization's online presence. When handling a patient's personal information in the healthcare industry, there should be a high level of privacy. For instance, health organizations must treat it fairly and solely for stated purposes, as well as securely store and send data. Researchers from the Journal of Diabetes Science and Technology (2021) depicted that the IEEE 2621 standard and its associated conformity assessment procedure have a value on cyber security progress in development, numerous industries that make income out of diabetes devices will participate in the standard and demonstrate conformance (Trisha Shang, Jennifer Y. Zhang, Joe Dawson, & David C, 2021).

Besides that, the client's private information must be protected at financial companies. The names, contact details such as phone and email addresses, and location details, for example. In education field itself, confidential and private data of students, staff, and school must be safeguarded and used for certain purposes promptly in all educational institutions and universities. If these security measures are violated, disciplinary measures ought to be in place. Higher education institutions are subject to a variety of cyber security dangers, not just those brought on by large corporations or nonprofit governmental agencies (Dioubate & Wan Daud, 2022).

Technically speaking, international collaboration on cybersecurity has been extremely successful in preventing attacks to interconnected systems and responding to those threats which is especially when considering the lack of precedent for the size and extent of the difficulties involved (Madeline Carr & Feja Lesniewska, 2020). In the aviation sector, protecting customer information is crucial, and it should only be used for those purposes. In addition, security measures must be in place to stop unauthorized access to passenger data. To control customer data globally, e-commerce needs, comprehensive data-protection rules. These rules make sure that any time customer data is gathered, shared, processed, or sent, it is done so legally.

Six ASEAN nations' legislative and policy frameworks for cyber security have been examined. As one can see, the majority of ASEAN nations have passed laws and policies to address issues such as platform openness by limiting platform owners' liability, combating cybercrime by creating laws that punish online wrongdoing, and protecting citizen personal data by creating laws and regulations to ensure citizen privacy (Jirapon Sunkpho, Sarawut Ramjan & Chaiwat Ottamakorn, 2018).

IV. CYBER SECURITY POLICIES AND EMPLOYMENT SYSTEM

Cyberspace has recently developed into a terrorist target zone. For many organizations, whether public and private, defending cyber security and preventing cyber terrorism are essential jobs. Organizations must comprehend how prepared for terrorism employees perceive themselves to be, as well as how prepared they are, according to objective assessments of hazards (Taewoo Nam, 2019). In this section we will emphasize real life cyber security attacks and the countermeasures that could been taken.

A. Real life cyber security attacks

Only a few of the cyber risks that can harm both public and private organizations include highly developed dangerous software, disruptive action by all respective individuals including organized crime, nationalist groups, and internet activists, as well as electronic cyber espionage activities (Taewoo Nam, 2019). Malaysia may gain from previous local hacking and cybercrime incidents that had place in the nation. The time is now to embrace blockchain technology for increased security as technology develops.

Based on New Straits Times (2022), due to a lack of adequate cyber security safeguards, many organizations are susceptible to cyber threats like malware, phishing, and ransomware. Malaysia had experienced numerous cyber-attacks just in the past year. These include a payment gateway data breach and the theft of personal data from a nationwide registration of the 22.5 million public who entrusted their data with the organizations. According to Sophos' State of Ransomware 2022 research, 79% of local organizations experienced ransomware attacks in 2021, which is much more than the 66.6% global average.

According to the Malaysia Cyber Security Strategy 2020–2024 report, cyber threats might cause the nation to suffer economic losses of up to RM51 billion. To stop this from happening in such a sensitive environment, strategic strategies, curated detection and response technologies, and cyber security awareness programs are required. Numerous cyber-attacks, such as the Internet transmission of viruses and worms, could damage the e-learning environment and endanger the data and the user. Additionally, because of universal connection, users' data may be acquired without their awareness or without unlawful access. The intellectual property may be attacked for instructional materials. The type of cyber-attack might occasionally take on different forms.

B. Countermeasures taken

There are few countermeasures that suggested when cyber security threats happen. We need to change our strategy from one of reaction to one of action. When an attack becomes clear, it's frequently too late. Businesses must search for dangers while presuming that they are compromised. Watch out for early indications of compromise. Two things stand out as early signs of compromise where the first is the use of credentials for remote access or administrative tasks outside of business hours, and the second is the use of system administration tools for spying.

Cybersecurity aspects, including workload, stress, teamwork, signal detection, decision-making, and attention study, and awareness are included in the field of human factors, which is the scientific application of these concepts (Robert S. Gutzwiller, Dan Cosley, Kimberley Ferguson-Walter, Dustin Fraze & Robert Rahmer (2019). Employees should react as soon as they can. Every second counts when a company is being attacked. An organization should spend more money on awareness and instruction across the board. Business leaders must educate employees about cyber security and encourage them to take cyber security training. They also should request for an assistance. In addition to the necessary tools and procedures, it is crucial for a company to inform its employees of the most recent security risks. Although we will never be able to perfectly secure our data, by adopting tools and procedure such as cryptography, firewall, use tools with simulated data and simulation tools, we could constantly lower the security risks and issues that happen (Machap, 2021).

Based on the research carried by the four-component approach which is action-related, advice-related, cognitive-type related, and lastly attitudinal-type fatigue offers a fresh theoretical conception with the main objective of attaining the best organizational cyber security results in application (Reeves, Delfabbro & Calic, 2021). The researchers said action-related is about fatigue brought on by strenuous or repetitive activity meanwhile advice-related is fatigue that brought on by difficult counsel, an abundance of information, or conflicting guidance. Cognitive-type related is the maximum number of cognitive resources that a person can commit to security issues. On the other hand, attitudinal-related is a negative attitude toward security concerns and a negative assessment of such worries.

V. THREATS AND CYBER SECURITY CHALLENGES

Since then, devices, computer networks, software, and the area that internet covers, for instance, the social media, emails have transformed each element of human behavior and presented innovative criminals with an endless stream of new chances for crime. Therefore, it should not be shocking that the security sector encompasses a broad range of actors who transcend well established organizational lines, including intelligence, policing, and defense organizations as well as policy divisions from various governmental tiers.

A. Employee

Initiatives led by the government and organizations should strive to enhance and expand cyber security capabilities as digital literacy or skill sets relevant to cyber security at the individual, group, and community levels, even though regular people are often not the primary focus of such training and the education (Taewoo Nam, 2019). Organizations must step up their efforts after security breach incidences by improving security behavior modification learning and training programs. Planning for cyber security should take the needs of the employers into great consideration. To fully understand the significance of cyber security awareness, internet users, especially the employees must have a clear understanding of the concept of awareness for the good of the organizations.

Relevant organizations have coordinated initiatives and efforts to raise the rate of awareness of cyber security, best practices, and safe internet use all over the Critical National

Information Infrastructure (CNII) including the public elements in order to ensure the deep implementation of cyber security awareness, education programs and acculturation. Employees might feel better prepared to confront with cyber security issues after obtaining training, making them feel less exposed. People might thus begin acting irresponsibly in regular security-related circumstances (A. Reeves, P. Delfabbro, & D. Calic, (2021).

Some of the most common issues and obstacles in the network are security threats from both inside and outside the firm, attacks brought on by end user ignorance, and how security measures are applied in the network (Machap, 2021). Before deciding if employee disengagement is attitudinal, cognitive, or a combination of the two, practitioners should identify whether cyber security advice or action has worn out the employees (A. Reeves, P. Delfabbro, & D. Calic, 2021).

B. Process

Accuracy, integrity, and safety of IT activities and resources will grow if control is successfully given to the organization's IT components because of their capacity to reduce errors, fraud, and network environment damage in that Malaysian organization. Additionally, it would guarantee the quality of IT facilities and lessen any potential harm to Malaysian firms' business strategies. At the same time, people and organizations of all sizes are being urged and held accountable for practicing cyber security. The establishment of new network-based cyber security centers will surely have a good impact on raising public awareness of cyber security issues and mobilizing resources to counteract cyber threats across organizational boundaries and professional disciplines. Since human mistake accounts for most cyber vulnerabilities, it is crucial to increase public knowledge of cyber security.

Cybercriminals are more common due to the epidemic and modern people's frequent online activity; this also includes an employee in an organization (Qi Xuan, 2022). Additionally, if individual users are viewed as capable and responsible, informing them about safe data and internet behaviors as well as privacy concerned technologies might be another measure taken in this strategy to increase cyber security. This strategy can also be used within corporations or organizations, for example by establishing password policies for employees (Fichtner Laura, 2018).

C. Technology

There are far too many IT resources and tools accessible today to aid a firm in maintaining their cyber security. The IT infrastructure and technology have continuously evolved and changed, just like the dangers. Therefore, Malaysian organizations must constantly be aware of and act upon any updates to IT infrastructure and technologies in accordance with digital security. The newest innovation in the technological world across all sectors is the digital signature. A digital signature is a collection of characters and numbers which represents the user's signature on an electronic document provided by a computer system (Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali & Mohd Norazmi bin Nordin, 2021).

Employees heavily depend on electronic or internet communication at work, where a massive amount of data is stored and exchanged back and forth. However, this method carries a higher risk because unauthorized individuals or fraudsters may acquire access to such information and utilize it in ways that are unethical for the government, private organizations, or a violation of individual privacy (Babayo Sule & Bakri Mat, 2019). The need for cyber security is greatest here. Cyber security is one of the core skills for Industry 4.0. Although Malaysia has numerous laws, norms, and policies for the benefit of people with disabilities, the provisions are not strictly followed. Despite the PWD Act being passed in 2008, PWDs are still regarded as one of Malaysia's most disadvantaged minority groups (Talib, R., Sunar, M., & Mohamed, R., 2019).

VI. CONCLUSION

In conclusion, employment system can be safer and reliable if all parties including the employer and the employee practices the best practice of keep confidentiality, integrity and availability of the organization’s employment system, networks and programs secured and understand how much risk that the vulnerabilities in cyber security directly or indirectly affect the organizations. Cyber-attacks not only occur in working environment, but it also occurs everywhere where the internet exists. Before the cyber-attacks happen, it is important for all the parties including organizations, family and friends to be attentive and aware of trending attacks that exists and always up to date with preventive measures to be taken by knowing the consequences of cyber-attacks towards us.

ACKNOWLEDGMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Systems & Network Security Project. This work was supported by University Utara Malaysia.

REFERENCES

Buja, A. G. (2021). Cyber Security Features for National E-Learning Policy. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1729–1735. https://doi.org/10.17762/turcomat.v12i5.2169

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Dioubate, B. M., & Wan Daud, W. N. (2022). A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(5). https://doi.org/10.6007/ijarbss/v12-i5/12924

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 76–92. https://doi.org/10.1177/00048658211003925

Fazlan Abdullah, Nadia Salwa Mohamad, & Zahri Yunos. (2018). Safeguarding Malaysia’s Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. *OIC-CERT Journal of Cyber Security*, *1*(1), 22–31. https://www.oic-cert.org/en/journal/pdf/1/1/114.pdf

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2). https://doi.org/10.14763/2018.2.788

Firkhan Ali Bin Hamid Ali1Mohd Zalisham Jali, Mohd Norazmi bin Nordin. (2021). Preliminary Study On It Security Maintenance Management In Malaysia Organizations. *PalArch’s Journal of Archaeology of Egypt / Egyptology*, *18*(1), 4061-4073. Retrieved from https://archives.palarch.nl/index.php/jae/article/view/6340

Gutzwiller, R. S., Cosley, D., Ferguson-Walter, K., Fraze, D., & Rahmer, R. (2019). Panel: Research Sponsors for Cybersecurity Research and the Human Factor. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 422–426. https://doi.org/10.1177/1071181319631383

Hamzah, M. A., Ahmad, A. R., Hussin, N., & Ibrahim, Z. (2019). Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies. *International Journal of Academic Research in Business and Social Sciences*, *8*(12). https://doi.org/10.6007/ijarbss/v8-i12/5251

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Computing Surveys*, *54*(11s), 1–35. https://doi.org/10.1145/3510410

Kunhibava, S., & Bakar, M. A. (2018, August 5). *Prospects And Challenges: Blockchain Space In Malaysia*. Https://Www.Academia.Edu/37184994/Prospects_And_Challenges_Blockchain_Space_In_Malaysia

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Machap, Dr. K., & Abulla Muaza. (2021). Use of network and cyber security tools to counter the security obstacles. Journal of Applied Technology and Innovation, 6(1). https://dif7uuh3zqcps.cloudfront.net/wp-content/uploads/sites/11/2021/12/07173349/Volume6_Issue1_Paper2_2022.pdf

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 538. https://doi.org/10.3390/s22020538

Mohamed Nawi, N. W., Alsagoff, S. A., Osman, M. N., Abdullah, Z., & Nazuri, N. S. (2022). The Influence of New Media on Cybersecurity and Law Implementation: A Qualitative Study. *International Journal of Academic Research in Business and Social Sciences*, *12*(6). https://doi.org/10.6007/ijarbss/v12-i6/13863

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Poor cybersecurity a top concern in Malaysia. (2022, November 10). New Straits Times. https://www.nst.com.my/lifestyle/bots/2022/11/849210/poor-cybersecurity-top-concern-malaysia

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Shang, T., Zhang, J. Y., Dawson, J., & Klonoff, D. C. (2021). Benefits of Conformity Assessment for Cybersecurity Standards of Diabetes Devices and Other Medical Devices. *Journal of Diabetes Science and Technology*, *15*, 193229682110181. https://doi.org/10.1177/19322968211018186

Sule, B. (2019, August 16). *Cybersecurity And Digital Economy In Malaysia Trusted Law For Customer And Enterprise Protection20190816 62421 I7dnx8*. Https://Www.Academia.Edu/40098075/Cybersecurity_And_Digital_Economy_In_Malaysia_Trusted_Law_For_Customer_And_Enterprise_Protection20190816_62421_I7dnx8

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018, March). Cybersecurity policy in ASEAN countries. In *17th Annual Security Conference* (pp. 1-7).

Tarhan, K. (2022, January 31). *How A Medium-Sized Country Ranks Higher In The Indexes For Cybersecurity: The Case Of Malaysia In The Context Of Legal And Administrative Regulations*. Https://Www.Academia.Edu/70039430/How_A_Medium_Sized_Country_Rankis_Higher_In_The_Indexes_For_Cybersecurity_The_Case_Of_Malaysia_In_The_Context_Of_Legal_And_Administrative_Regulations

Qi Xuan, N., & Dr. Intan Farahana Binti Kamsin. (2022). Enhance Public Cybersecurity Awareness By Understanding Cybersecurity And Cyberthreats. Journal of Applied Technology and Innovation, 6(3). https://dif7uuh3zqcps.cloudfront.net/wp-content/uploads/sites/11/2022/06/09143148/Volume6_Issue3_Paper3_2022.pdf