Digital Security Challenges Faced by Business Organizations

Raenu Kolandaisamy, Heshalini Rajagopal
Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia

Indraah Kolandaisamy
School of Business Management, University Utara Malaysia 06010 Sintok, Kedah

Glaret Shirley Sinnappan
Tunku Abdul Rahman University of Management and Technology, Kuala Lumpur, Malaysia
E-mail: raenu@ucsiuniversity.edu.my

Abstract

Over the decades, the forms of cyber-attacks have evolved from disruption level, cybercriminal, followed by cyber espionage and lastly threatening level. Digital security has played a significant role in protecting enterprises from any form of cyber-attacks, especially in today's era of digitalization. Aligning with the global effort in emerging the concept of Industrial Revolution 4.0 (IR4.0) in organizations, where sensitive data and confidential information can be accessed at a fingertip of an employee. This paper discusses the difficulties of implementing digital security solutions in an enterprise in terms of external potential cyber threats, internal cyber security roadblocks within the organization and how Covid-19 pandemic imposed challenges towards cyber security in the organizations.

Keywords: digital security, cyber security, cyber-attacks, cybercriminal, cyber espionage, business organizations

1. Introduction

The Information System has changed our lifestyle over the past decades among banking systems, education, transportation, business, tourism, shopping. The rise of internet consumption has dramatically increased by organizations and individuals with massive global international trade and changes of human interaction in the young generation. Digital economy can refer to integration of new business models, goods, services and markets established on a basic business infrastructure with digital technologies. Digital technologies can be defined as consolidation of communication, computing, information, and connectivity technologies that are driven by storage, software applications, sensors and bandwidth to the next generation of digital economy through cloud computing [1].

The rapid development of science and technology is far more than that such as the internet of things (IoT), artificial Intelligence (AI), augmented reality (AR), drones, additive manufacturing (3D printing), robotics and others. These latest technologies work from extracting data from sensor conditions of physical devices, spreading and storing it rapidly on cloud to analyse it in real time by using advanced big data analytics for generating useful information of integrating services, products and processes, and making decisive influence on existing business models. Meanwhile, approximately 90% of business managers in developed countries like the U.K. and U.S. forecast information technology and digital technologies contribute strategic values to the entire economy in the future. On the other aspect, information technologies will uncover a variety of new threats of cyber security challenges and risks when more companies foster innovation by increasingly popularizing new digital technologies, while security information technologies are changing and evolving to become a complicated threat (cyber security). Furthermore, information security cases might have caused a minor technical problem 10 or 15 years ago, but today advanced and intentional cyber attacks are challenging us that might cause large-scale events as a result of direct and indirect consequences affecting business's strategy and competitive advantage [2].

Browsing the internet, reading digital books, social networking, searching content, and online shopping are transforming our lives to better, efficient and productive ones. However, most of the netizens and organizations lack cyber security awareness and relevant knowledge of internet hazards. Individuals and business organisations have limited knowledge to protect their devices and servers from cyber hazards such as financial fraud, sensitive information theft, website spoofing, Internet of Things (IoT) hacking, malware, distributed denial of service attack (DDoS) as well as ransomware. Cyber hazards come from the work of hackers also known as "black hats" who committed cyber crime on their own or with an organized criminal group. Large-scale breach of cyber security has been rated by the World Economic Forum as one of the five most

critical threats confronting the world today where the scope of threat globally is spreading rapidly and cost an estimated US$6 trillion by 2021 [2]. Nevertheless, studies show that installing protective tools on the computers from factories does not maximize cyber security generally. Hence, this paper examines the challenges faced while implementing cyber security solutions into organizations' systems in various different perspectives.

2. Result and discussion

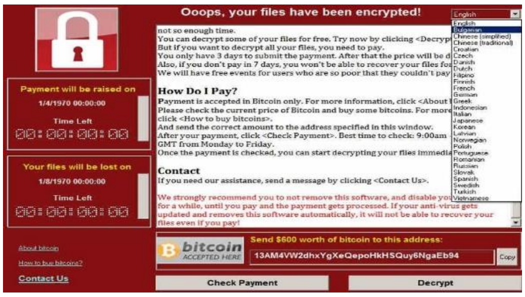
According to the Internet Crime Report published by the Cyber Division of the Federal Bureau of Investigation (FBI) in the year of 2020, losses exceeding USD 29 mil resulted from 2,474 ransomware attacks registered worldwide has been recorded [3]. The fact that cyber crimes against enterprises have increased tremendously over the years has shown that the digital security systems or practices within the organizations still remained susceptible and vulnerable towards cyber attacks in any form or even worse, could not keep up with the growing pace of these cyber threats. Thus, the roadblocks or difficulties to carry out the implementation of the cyber protection have to be discussed thoroughly in terms of external cyber hazards, internal cyber security challenges in organization and challenges of digital security during Covid-19 pandemic in order to improve, correct and make changes towards the current situation of cyber security support in the right direction.

2.1. External Potential Cyber Hazards

The Internet has improved the standard of living of IoT users, but every pillar has two sides. Everything can be done smoothly by one click as the same goes with cybercrime. That could so easily invade valuable information of individual and business organizations by various cyber hazards such as malware, phishing, distributed denial-of-services attack (DDoS), man-in-the-middle attack (MMIT), ransomware and insider threats [4]. Every cyber attackers' intentions are different, but mostly demanding for money, financial information, personal information and even the business infrastructure. Cyber attacks target individuals and business organizations that have less cyber security awareness and protection tools because they always have key assets to be exploited by criminals. According to "PricewaterhouseCoopers survey", organizations that undergo cyber attack relevant matter vanished 2.1% of its value and lost more than 1.6 billion USD per case on average [2]. Understanding the motive of cyber attackers and hazards is essential for internet users to prevent financial loss and irreversible consequences. There are three aspects of motive to be proven as crime which are motive, means, and opportunity that can be treated as a conventional crime. Means refer to an attack tool or technical expertise to execute the attack, motive is the aims, intention, purpose or reason of the attacker selecting a target, opportunity can be seen as a timing, vulnerability and weakness in the network of the target [5].

Ransomware is a kind of malicious software that encrypts files of business organizations by demanding ransom in exchange for a decryption key [6]. It is very difficult to detect hijacked files and data before a cyber attacker initiates the attack. There are only 2 options for users to solve the problem which are to pay ransom in exchange for a decryption key to retrieve files and data or disconnect the internet and format the computer [4]. However, it is nearly impossible for internet-based business organizations to get rid of ransomware by formatting all data in digitized generation because it is the foundation and infrastructure of the company. In 2012, Reveton is one of the recognised ransomware trojans that ransom nearly $130,000 fines from victims who believed that they have been charged for participating in illicit online activities. Business organizations weren't too worried about the attack because it was affecting mostly individuals. By the end of 2016, an estimated $1 Billion was paid to the ransom hackers from Cryptorlocker and CryptoWall. It gave a huge profit trajectory to the hackers, something big known windows exploits were on the way from the National Security Agency (NSA). The worst and largest ransomware attack that ever happened before in 2017, "WannaCry" (Fig. 1) ransomware attacked more than 230,000 computers of various industries which were universities, government organization, hospital, bank, logistic, telecommunication companies, railways companies and business organizations across 150 countries [7]. According to research from "SonicWall Capture Labs", ransomware cases have risen by 20%, with up to 121 million attacks recorded around the world in the first half of 2020 [8].

Working of ransomware (Fig. 2) will be introduced into 4 steps. First, the ransomware starts with an unsolicited email usually designed to trick the victim into clicking on an attachment or visiting a webpage. Second, ransomware leverages flaws in the computer's command-and-control server and forces it to download a public key for running ransomware code. Third, important data is encrypted on the system and demands a ransom payment using cryptocurrency by providing ransom fee instructions. Lastly, the decryption key will be given by the attacker once the ransom is paid [4].



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be d
Also, if you don't pay in 7 days, you won't be able to recover your files fo
We will have free events for users who are so poor that they couldn't pay

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About
Please check the current price of Bitcoin and buy some bitcoins. For more
click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am
GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immedia

Contact

If you need our assistance, send a message by clicking <Contact Us>.

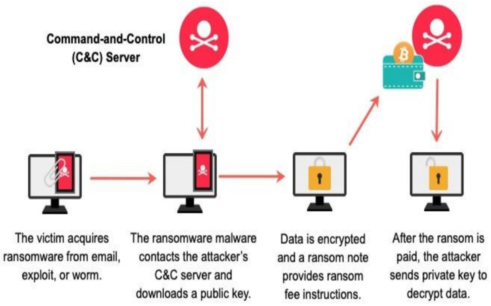
We strongly recommend you to not remove this software, and disable yo
for a while, until you pay and the payment gets processed. If your anti-virus gets
updated and removes this software automatically, it will not be able to recover your
files even if you pay!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

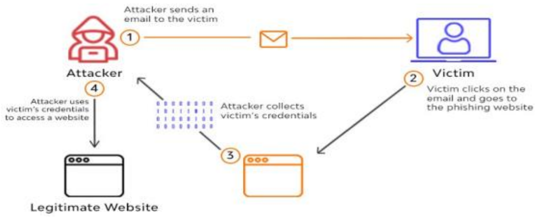
Fig. 1 Activation of "WannaCry" on victim's computer



Command-and-Control
(C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware malware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends private key to decrypt data.

Fig. 2 Ransomware mechanism

Phishing attacks (Fig. 3) is a social engineering technique to bypass computer security and human defence by using social networks, emails, mobile apps, instant message, business email compromising or search engine poisoning to steal user's data, sensitive information, credit card number and code, as well as login credentials to make the victim perform an action. There are more than 30% of cybercrime caused by phishing attacks and cost at least 8 billion USD according to Verizon Data Breach Investigation (DBIR). There are some technical countermeasures to mitigate risk of phishing such as anti-phishing, email malware detection, data loss prevention and spamming tools. However, it's not effective because these technical countermeasures are unable to analyze and differentiate between phishing and general email. Furthermore, business organizations provide phishing attack awareness training to their employees against phishing techniques, tactics, and procedures (TTPs) through email security guidelines and standard operating procedures to increase cyber awareness [9].



Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Legitimate Website

Fig. 3 Phishing attack mechanism

Distributed Denial of service attack (DDoS) attack is one of the most common cyber crimes faced by business organizations when a group of botnets, server or numerous connected internet devices flood the capacity limit and resources of a targeted system as a result in service degradation and unavailability by disrupted normal traffic. Attacker will control his resources to overwhelm the capacity limit of the server by sending numerous requests to the targeted IP address of the website in a short time that trigger a crash. DDoS attacks could stay as long as 24 hours and up to days to retain access to the unavailability of the company's server that lead to reputation damage and profit minimization. There are vulnerabilities in the system that are exploited by the hackers although various protections and prevention are applied.

DDoS attacks (Fig. 4) are conducted with private networks of internet-connected machines and any kinds of IoT devices. Attackers can remotely control the networks that are constituted by computers and devices that are malware infected. These infected devices can be called bots (or zombies), and a botnet where a group of bots is connected in a network. Attackers are allowed to send attack instructions to each bots when the botnet has been established. When each bot sends requests to the victim's IP address, possibly causing the server of the website to be down where limit traffic is triggered during a short period as a result of denial-of-service to normal traffic. Because the server is difficult to identify attack traffic and normal traffic from each bot is considered a legitimate internet device [10].

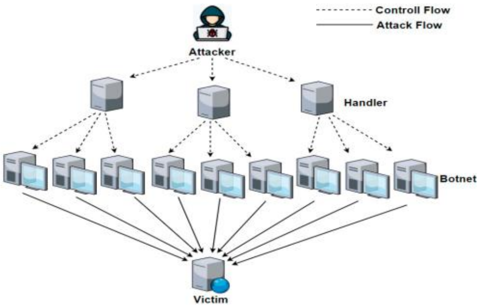


Fig. 4 DDos attack mechanism

Types of DDos Attack

- Ping of Death (POD) attack
  POD attack exploits the particular characteristic based on the maximum size of the packet of transmission control protocol (TCP)/ internet protocol (IP) can be up to 65,535 bytes in normal cases. Generally, in the case of a large IP packet, it will be splitted into numerous fragments and reassembled into a complete packet to the recipient host. However, POD attack exactly exploits the reassembling packet size of 65,535 bytes greater than its maximum to maliciously manipulate overflow of memory allocated as a result of denial of service[11].
- Hypertext Transfer Protocol (HTTP) Flood Attack
  HTTP flood attack is another method of resource consuming by manipulating the HTTP GET and HTTP POST requests while connecting with the victim's machine [12]. HTTP works as a request-response protocol and designs to allow communications between servers and clients. HTTP GET and POST are the two most common methods where GET requests data from a particular resource and POST sends data to a server to update or create a resource [13].
- Domain name system (DNS) Flood Attack
  DNS is the "contact list" of the internet which allows devices able to view the content of websites. It sends a huge amount of DNS requests to the target device in order to overload it and reduce the speed of traffic. Attack will be done by the botnet to generate a large volume of traffic [12].

Cloud computing attack (CCA) is a malicious activity that involves data breaches, manipulating, account hijacking or eavesdropping from a user's virtual machine on the physical server by injecting malware from the hacker. Once the cloud system is deceived, hacker can gain unauthorized access to the user's cloud storage without permission and awareness. CCA could be conducted by various methods such as structured query language (SQL) injection attack, DDoS attack, malicious insider, side channel attack, man-in-the-middle (MITM) attack and abuse of cloud services. Cloud computing attack is the most economically significant threat in the world of virtualization technology, confidential data breach is one of the key diminish potential revenue loss and customer trust [11]. In fact, a massive cyber attack in Sweden in July 2017, a high confidential data stored at cloud system was breached, causing irreversible consequences that exposed national secrets, national security, international wrongdoing, and resignation of ministers. In fact, a massive cyber attack in Sweden in July 2017, a high confidential data stored at cloud system was breached, causing irreversible consequences that exposed national secrets, national security, international wrongdoing, and resignation of ministers. In June 2017, British Airways cloud system was being disrupted by hackers as a result of financial loss at 114 million EUR due to over 100 flights being cancelled from London airports [2].

SQL injection (Fig. 5) attacks is a common attack where an attacker inserts malicious code to unauthorized access to a backend database to gain sensitive information that was not intended to be disclosed or private company data. Generally, SQL injection attacks require an attacker to figure out the vulnerability of a webpage or web application to perform unauthorized access without an official account. For example, a logical user's account coupled with usernames and passwords that are registered at the database, attacker could input malicious code like username = '1' or 2>1 --' and password = '111' to bypass source code of the web application [14].

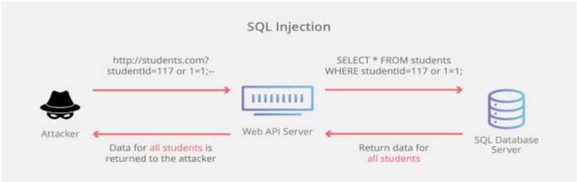


Fig. 5 SQL Injection mechanism

MITM (Fig. 6) occurs when an attacker establishes independent connection with separate ongoing conversations to different third parties by misleading them with the aim to inject, steal or exchange information to manipulate the result. Third parties are not aware that the attacker has control over the ongoing conversation between both parties. All of the message sent by one party to another will go through the attacker and it allows the attacker to tamper the information to mislead both parties [14].

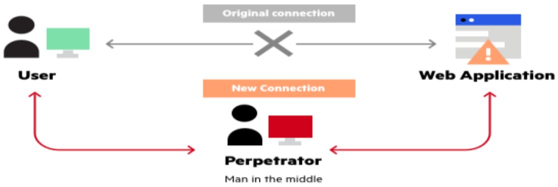


Fig. 6 MITM mechanism

2.2. Internal Cyber Security Challenges within the Organization

Other than external cyber security challenges in the form of various cyber threats, there are seven internal challenges in implementing or improving the cyber security in an organization where these challenges could be grouped into three different categories or foundations for the organizations which are the three pillars of People, Process and Technology [6]. Indeed, human resources or employees are important assets to the organization, however, also one of the internal factors that drive the organization to the risks of exposing them to the emerging and evolving cyber threats when the employees are lacking cybersecurity skills, demonstrating irresponsibility and conducting human error while dealing with sensitive data and processes [6]. Firstly, the lacking of cybersecurity skills is said to be one of the challenges of cybersecurity in an organization and getting worse four years in a row since 2017 where this crisis has impacted almost 70% of the organizations globally according to the fourth annual global study by both the cybersecurity professionals, the Information System Security Association (ISSA) and independent industry analyst firm, the Enterprise Strategy Group (ESG) [15]. In fact, there are numerous factors that lead to such cybersecurity expert shortage crisis which could impose significant cybersecurity risk to the organizations, they are mainly due to global worker shortages, limited hands on skills as well as experience in handling cyber attacks and threats, the increasing workload of employee resulting in lesser time to acquire the relevant skill set, the incompetence of the employees to learn or utilize the cybersecurity technologies to the fullest potential, etc [16]. Thus, it is clearly evident that lack of skills in cybersecurity is one of the most challenging concerns in implementing cybersecurity measures under the pillar of 'People' within the organizations. Besides cybersecurity talent shortage, the irresponsible behaviour of the employees towards cybersecurity is also one of the challenges faced by the organizations in implementing the relevant measures. Most of the employees in an organization would intend to push the responsibility of the IT staff only, whereby the cybersecurity implementation is not solely IT departments responsibility, but all employees from operational level to management level within the ecosystem of the organization [17]. Thus, with such irresponsible behaviour, the employees tend to put lesser attention onto the data handling which leads to the ignorance attitude towards the basic cyber security practices and possibly violating the compliances of cyber security. Not only that, employees' careless work behaviour such as inappropriate sharing confidential information with third parties without permission, inappropriate use of IT resources, losing their own devices storing company data, etc. could lead to a significant financial loss to the organization [18]. This could be evident when the result from the IT Security Risks Survey 2017 has indicated that almost 11% of the cyber attack incidents are due to careless and uninformed employees as shown in Fig. 7 below [18]. Hence, proven that the irresponsible act of the employees could definitely lead to hard time for the organization to implement the cybersecurity measures.

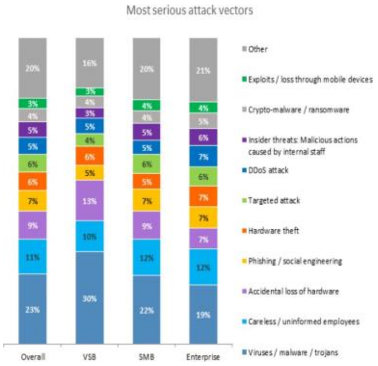


Fig.7 Most serious cyber attack vectors over the 12 months in 2017.

Furthermore, human error has also contributed as an obstacle towards the implementation of digital security in an organization [6]. This could be proven from a survey conducted by IBM in 2018, indicating that the misconfiguration of cloud servers due to human error is the biggest risk in cyber security in cloud computing with 62% of survey participants made up of IT and security professionals, while 55% of them noting misuse of employee credentials and improper access as one of the human error contributing to challenges while implementing cyber security measures, followed by insecure interfaces at 50% [19]. In fact, misconfiguration of systems usually allows cyber criminals to access large data platforms consisting of usernames, passwords, credit card data, health data, national identification numbers, email addresses, etc. which could possibly be used to request for ransom from the organizations. For example, one of the significant cyber attack incidents happened due to misconfiguration of system and human error in 2018, where a well-known marketing firm in the US, Exactis was reported leaking approximately 340 million files to the public including sensitive personal details ranged from national identification number to hobbsies by making them available through a server accessible to anyone [20]. This incident has definitely shown that human error within an organization especially involving data handling and system configuration will definitely lead to big loss to the organizations regardless of financial or reputation.

The processes, which is the second pillar of an organization, has played an important role in cybersecurity implementation. There are three cyber security challenges identified under the pillar of 'Process' in a recent research, which include the lack of implementation plans for cyber security measures execution, the misplaced human resources and the lack of budget allocated for cyber security efforts within the organization [6]. The readily compliance and regulations governed nationally such as cyber security guidelines used in Malaysia including Information Technology Instructions 2007, ICT Security Policy 2010, Electronic Government Act 1987, Public Sector Cyber Security Framework 2016, etc., would need a good implementation plan within the organization in order to apply the guidelines into processes and enforce the cyber security strength of the organization [6]. However, most of the organizations do not emphasize cyber security planning which ultimately leads to a higher risk of monetary loss and reputational damage [21]. The mentioned phenomenon could be proven by the results of the survey conducted by The Department for Digital, Culture, Media & Sport (DCMS) in the UK on 1,500 businesses from October to December 2017, where only 38% of the businesses is aware of the new incoming data protection law, while only 27% from these businesses have made the changes on the organization processes and less than half of these businesses made changes to the cyber security practices within the organization, leading to a total of 43% of these businesses in the UK experienced cyber threats in 2017 [22]. The lack of implementation plan could involve cyber security governance, protection measures, hardware maintenance plan, incident response plan, evaluation plan, documentation including policies, Standard of Procedures (SoP), Work Instruction (WI), etc. where the effectiveness of the cyber security implementation is directly affected by the quality of these elements [21]. Therefore, detailed construction of the implementation plan is indeed important to ensure the cyber security measures are being implemented and executed accordingly in order to reduce the risks of exposing the cyber physical asset of the organization towards potential cyber hazards.

The next digital security challenge in an organization under the pillar of 'Process' is poor human resource management. For instance, new arrangements for cyber security talents in the workplace due to promotion to managerial positions, assignments to new departments or even the failure to retain cyber security talent would lead to the reduction of trained and experienced talents that could counteract cyber threats in an organization [6]. Due to talent loss, more time would need to be consumed to acquire capable talents, to train and nurture the replacement, etc which would cost a knowledge gap in terms of cyber security in the organization, leading to the risks of cyber invasion [23]. In fact, a survey conducted on cyber resilience by IBM Security and the Ponemon Institute has shown that 75% of the survey respondents found it difficult to hire and retain skilled cyber security professionals in respective organizations, while 48% of them has also pointed out the complexity in operation due to various type of security tools being implemented, causing the weakening in cyber resilience due to the skill and abilities gap between existing talents and tools deployed within the organization [24].

The sixth challenge in digital security within an organization is the limited budget allocated for the implementation and enforcement [6]. A detailed cyber security budget allocation should include risk analysis cost, technology acquisition or software licensing costs, training charges, insider threat reduction cost, etc. to reduce the potential risk of cyber internal breach and external threats [25]. However, most of the top management in the organizations especially small and medium enterprises do not prioritize cyber security because they would be willing to maximize the profitability instead of spending on cyber protection measures for incidents that may not happen, but they did not consider the possibility of cyber security failures which would cost the organizations even more [26]. For example, RiskIQ estimated financial loss of $17,700 per minute will be imposed on the victims due to phishing attack while Accenture estimated Malware rates up to $2.6 million at most and Ransomware rates up to $646,000 on average [27]. Not only that, organizations with improper cyber security could also be fined as it would induce insecurity within users, for instance, Google was fined at a cost of $57 million in 2019 due to the failure in complying with General Data Protection Regulation (GDPR) in France [28]. Thus, limited budget allocation as a roadblock in cyber security of an organization would definitely cause larger amounts of financial and reputational losses in the future as the risks from organizations internally or cyber threats externally are not being mitigated sufficiently.

Lastly, business organizations are facing cyber security challenges when the technology advancement is evolving too fast, so does the advancement in cyber threat vectors [6]. In fact, the cyber threats are characterized as asymmetrical and multi directional, making the organizations being reactive instead of proactive while facing the new form of cyber attacks[6].

Also, as the world is currently accelerating towards IR4.0, the organization especially in manufacturing industry which adopting technologies such as Robotics and Automation (R&A), Artificial Intelligence (AI) and Machine Learning (ML), Big Data Analysis (BDA) and Cloud Computing (CC), etc, where these technologies adapted are actually associated with the risks of being attacked by cyber criminals [29]. For example, Booz Allen Hamilton has pointed out the largest potential risk of AI and ML algorithms that worry the most is the possibility of leaking the training data to cyber criminals as this training data is sufficient enough to rebuild the original AI model via reverse engineering [30]. Thus, it is clearly shown that the benefits from ever evolving technologies aligning with IR4.0 are always associated with greater risk of cyber hazards invasion.

Recommendations are proposed in terms of the three main pillars which are people, process and technology, in order to help overcome the internal challenges faced by the organizations while implementing cyber security measures.

Firstly, human resources (HR) directors should play a key role or even a leader to keep the organizations safe from internal cyber breaches and employee-imposed cyber threat risks. As a HR director, a HR team should be formed to work with the IT or cyber security department to align the expectations ensuring the digital security measures and policies to be implemented is practical, ethical and appropriate. Besides, the HR director and the team should also take ownership of the security risk posed by employees by providing sufficient education regarding the impact of the employees behaviours towards the cyber security of the organizations as well as identifying employees who may be insiders allowing risks of external cyber threats to be imposed on the company. Overall, the HR team plays a vital role in shaping the workplace culture where the employees are following the reviewed cyber security measures and policies to help reduce the risks of cyber attacks. [31]

Secondly, in terms of processes, the management systems within the organization are vital in combating cyber security breaches. A proper management system must be adopted to ensure all the employees are aware of their duties and responsibilities as well as to adequately manage the level of competence and interest of the employees in cyber security. Besides that, a series of enterprise cyber security governance activities should be conducted from time to time to continuously improve the strength of the cyber security, where the activities include adopting enterprise risk management (ERM) to prevent data loss, and also, conducting threat, vulnerability and risk analysis tests within the organization to access the sustainment of the cyber security governance. Moreover, the policies, SOP and WI related to cyber security measures and practices should be comprehensive enough and made available to every employee to ensure these guidelines or documents are clear and easy to understand to avoid miscommunication as well as guiding the employees in their decision making process when facing issues

like cyber attacks attempts. Vendor management is also one of the important processes to be focused on regarding cyber security because the vendors may potentially serve as a medium for external cyber threats invading the organizations, thus, it is important to ensure the vendors engaged are equipped with the same level of security. [32]

Lastly, in the aspect of technological advancements, organizations are suggested to adopt AI-based cyber security management systems where the systems allow to leverage up-to-date global cyber security knowledge and industry specific threats to make significant prioritization decisions as well as prompt incident response when exposing to cyber threat, keeping track of all organizations' IT assets in a domain to perform breach risk prediction and generating comprehensive reports on recommendations and analysis of the decisions proposed to all the involved stakeholders. [33]

3. Conclusion

In this paper, cyber security challenges faced by the business organizations have been discussed and analyzed in two different perspectives including the external potential cyber threats and internal factors within the organizations. Notable external cyber hazards such as the Ransomware, Phishing Attacks, DDoS Attacks as well as Cloud Computing Attacks comprises SQL Injection Attacks and Man-in-the-middle have been introduced and their mechanism also have been discussed in this paper. Seven internal cyber security challenges within the organizations have also been highlighted in terms of three different elements which are people, process and technology, where by the challenges discussed include the lack of cyber security skills, irresponsible behaviour of employees, human error, lack of digital security implementation plan, poor human resource management, constraint of budget allocation for cyber security implementation and lastly technology advancement. Indeed, both the internal and external cyber security obstacles faced by the organization have allowed many digital security breaches and invasions to happen, which leads to critical negative impacts to the organizations, corporate and national such as breach of trust, data, privacy, financial or economical losses as well as the damage of reputation and public image. Therefore, further broad researches and detailed studies on cyber security especially the method of combating cyber threats and enhancing the strength of cyber security in organizations are recommended so that the readers could be provided with useful insights and ideas as well as emphasizing the importance of everyone's role in ensuring the success of implementing effective and efficient digital security measures in the organizations to instill the supportive behaviours and foster the cyber security culture within the companies.

References

1. M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, pp. 1–16, Feb. 2020.
2. M. Spremić, and A.Šimunic. Cyber security challenges in digital economy, Proceedings of the World Congress on Engineering, vol.1, pp. 4-6, Jul. 2018.
3. Internet Crime Complaint Center (iC3) Internet Crime Report 2020, Federal Bureau of Investigation. Accessed: Aug. 26, 2021. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
4. S. Mohurle and M. Patil, A brief study of wannacry threat: Ransomware attack 2017, International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 1938-1940, 2017.
5. A. Abhishta, M. Junger, R. Joosten, and L. J. M. Nieuwenhuis, A Note on Analysing the Attacker Aims Behind DDoS Attacks, Intelligent Distributed Computing XIII, Springer International Publishing, pp. 255–265, Jan. 2020.
6. C. S. Teoh, A. Kamil Mahmood, and S. Dzazali, Cyber Security Challenges in Organisations: A Case Study in Malaysia, 2018 4th International Conference on Computer and Information Sciences (ICCOINS), Aug. 2018
7. C. Adams, Learning the lessons of WannaCry, Computer Fraud & Security, vol. 2018, no. 9, pp. 6–9, Sep. 2018.
8. B. Hellard, 121 million ransomware attacks recorded in the first half of 2020, Itpro.co.uk, Accessed: Aug. 26, 2021. [Online]. Available: https://www.itpro.co.uk/security/ransomware/356567/1212-million-ransomware-attacks-in-the-first-half-of-2020
9. H. Shahbaznezhad, F. Kolini, and M. Rashidirad, Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?, Journal of Computer Information Systems, pp. 1–12, Oct. 2020
10. M. Aamir and S. M. A. Zaidi, DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation," Int. J. Inf. Secur., vol. 18, no. 6, pp. 761–785, Apr. 2019.
11. G. Levitin, L. Xing, and H. Huang, "Security of Separated Data in Cloud Systems with Competing Attack Detection and Data Theft Processes, Risk Analysis, vol. 39, no. 4, pp. 846–858, Oct. 2018.
12. L. Visalatchi, P.Yazhini, and M. Scholar, The survey DDoS attack prevention and defense technique, International Journal of Innovative Science and Research Technology, vol. 5, no. 2, pp. 65-68, Feb. 2020.
13. HTTP Methods GET vs POST, W3schools.com, Accessed: Aug. 28, 2021. [Online]. Available: https://www.w3schools.com/tags/ref_httpmethods.asp
14. N. Amara, H. Zhiqui, and A. Ali, Cloud computing security threats and attacks with their mitigation techniques, 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 244-251, Oct. 2017.
15. Help Net Security, Cybersecurity skills shortage still the root cause of rising security incidents, Accessed: Aug. 28, 2021. [Online]. Available: https://www.helpnetsecurity.com/2019/05/14/cybersecurity-skills-shortage-causes-security-incidents/
16. J. Oltsik, ESG Research Report - The Life and Times of Cybersecurity Professionals 2020, ISSA, Accessed: Aug. 28, 2021. [Online]. Available: https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf
17. Cybersecurity regained: preparing to face cyber attacks, Ernst and Young (E&Y). Accessed: Aug. 28, 2021. [Online]. Available: https://pdf4pro.com/view/cybersecurity-regained-preparing-to-face-cyber-attacks-ey-559d48.html
18. "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky Daily. Accessed:Aug. 28, 2021. [Online]. Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security/
19. Kolandaisamy, R., Noor, R. M., Zaba, M. R., Ahmedy, I., & Kolandaisamy, I. (2019, July). Markov chain based ant colony approach for mitigating DDoS attacks using integrated vehicle mode analysis in VANET. In 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP) (pp. 1-5). IEEE.
20. T. Collins, Exactis leaks the private details of 340 MILLION people to cyber criminals, including their phone numbers and home addressees, in a one of the biggest security breaches of its kind, Mail Online, Accessed: Aug. 28, 2021. [Online]. Available: https://www.dailymail.co.uk/sciencetech/article-5900071/Marketing-firm-Exactis-leaks-340-million-files-containing-private-data.html
21. S. Ursillo and J. C. Arnold, Cybersecurity Is Critical for all Organizations – Large and Small, IFAC, Accessed: Aug. 28, 2021. [Online]. Available: https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-larg e-and-small
22. The Department of Digital, Culture, Media & Sport (DCMS), "New figures show large numbers of

businesses and charities suffer at least one cyber attack in the past year," Gov.uk, Accessed: Aug. 28, 2021. [Online]. Available: https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businesses-and-charities-suffer-at-least-one-cyber-attack-i n-the-past-year

23. Cipher, What Causes Cyber Security Projects to Fail?, Accessed: Aug. 28, 2021. [Online]. Available: https://cipher.com/blog/what-causes-cyber-security-projects-to-fail/
24. Help Net Security, 77% of orgs lack a cybersecurity incident response plan, Accessed: Aug. 28, 2021. [Online]. Available: https://www.helpnetsecurity.com/2019/04/12/cybersecurity-incident-response-plan/
25. Kolandaisamy, R., Subaramaniam, K., & Jalil, A. B. (2021, March). A Study on Comprehensive Risk Level Analysis of IoT Attacks. In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) (pp. 1391-1396). IEEE.
26. S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," Journal of Organizational Computing and Electronic Commerce, vol. 28, no. 3, pp. 269–282, Jul. 2018.
27. J. Fruhlinger, "Top cybersecurity facts, figures and statistics," CSO Online, Accessed: Aug. 28, 2021. [Online]. Available: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
28. R. Dillet, French data protection watchdog fines Google $57 million under the GDPR, Tech Crunch, Accessed: Aug. 28, 2021. [Online]. Available: https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/
29. Baytamouny, M., Kolandaisamy, R., & ALDharhani, G. S. (2022, April). AI-based Home Security System with Face Recognition. In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1038-1042). IEEE. [30]. M. Korolov, How secure are your AI and machine learning projects?,CSO Online. Accessed: Aug. 28, 2021. [Online]. Available: https://www.csoonline.com/article/3434610/how-secure-are-your-ai-and-machine-learning-projects.html
30. Alt, R. (2021). Digital transformation in the restaurant industry: Current developments and implications. Journal of smart tourism, 1(1), 69-74..
31. Putting human resources at the heart of cyber security, PA Consulting. Accessed: Aug. 28, 2021. [Online]. Available: https://www.paconsulting.com/insights/putting-human-resources-at-the-heart-of-cyber-security/
32. The three-pillar approach to cyber security: processes are crucial, Det Norske Veritas. Accessed: Aug. 28, 2021. [Online]. Available: https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-processes-are-crucial-162890
33. Using Artificial Intelligence in Cybersecurity, Balbix. Accessed: Aug. 28, 2021. [Online]. Available: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Authors Introduction

Dr. Raenu Kolandaisamy

He received his PhD from the Faculty of Computer Science & Information Technology, University Malaya in 2020. He is currently an Assistant Professor in UCSI University, Malaysia. His research interest areas are Wireless Networking, Security, VANET and IoT.

Dr. Heshalini Rajagopal

She received her PhD and Master's degree from the Department of Electrical Engineering, University of Malaya, Malaysia in 2021 and 2016, respectively. Her research interest includes image processing, artificial intelligence and machine learning.

Dr. Indraah Kolandaisamy

Dr. Indraah A/P Kolandaisamy is a senior lecturer in School of Business Management, College of Business, Universiti Utara Malaysia.

Dr. Glaret Shirley Sinnappan

Dr. Dr. Glaret Shirley A/P Sinnappan holds the position of Assistant Professor in the Department of Information and Communication Technology at Tunku Abdul Rahman University College.