Security Challenges

A comprehensive Computer System Security report of the Security Challenges faced by SME's

Student:

Srikanth Shilesh Pasam (10387794)

Aniket Nilegaonkar (10525461)

Teacher:

Gordon Reynolds

Course:

Computer System Security – B9IS103 – CA 2

Index

Introduction

In this world of technology, both small and large enterprises are moving towards adopting and utilising technology in their organisational process, but there are various challenges and obstacles which are generally faced by Small and Medium-sized Enterprises (SMEs) (Hassan, 2020). SMEs are a category of small and medium-sized businesses, which are limited in some resources and have a smaller number of clients or customers. In this context, there are various industries which have the fastest-growing SMEs such as dentistry, engineering services, physicians' clinics, hotel or motels, legal offices, and so on. There is a high risk of malicious and cyber-attacks in the small and medium-sized enterprises as well as in well-built organisations. In this case, smaller companies are consistently producing, storing and utilising data in a huge amount which increases the risk of getting hacked or breached. Nowadays, the small and medium-sized companies are producing a large amount of data which makes it easy for a hacker to attack or intrude (Lee, Che-Ha and Alwi, 2020).

It is a big challenge for SMEs to enhance their security as the large enterprise maintains its security system, which can decrease the risk of hacking attacks. The most common category of hacking attacks in the business includes phishing, malware, Man in the Middle, Denial of Service (DoS) attacks and SQL injections (Rauch *et al.*, 2020). These attacks can be made internally or externally. In addition to this, the intrusion or hacking attacks can also decrease the value of the company in the marketplace; along with this, it also breaks the trust between the clients and the organisation. In this assessment paper, two topics have been selected for the further explanation in which the first is about challenges related to data theft and

data breach and the second topic pertains to challenges related to the risk of malicious threats from cybercriminals and non-implementation of ISO 27001:2013 standards. In this report, the main issues relating to data security in the small companies have been identified to find the possible solution for preventing these situations.

Challenges Related to Data Breach

There are various challenges which are being faced by small and medium-sized enterprises. In addition to this, some of the challenges related to information security are mentioned in following paragraphs, along with recommendations which can be utilised in order to increase the value in the marketplace and retain the clients or customers.

There are several challenges and obstacles in the way of small businesses. The first and the most important task are to build bond and trust between the client and the company, but it is not possible without enriching the security in the organisation. In the context of security, it is necessary for any organisation for retaining its business and market value. If an incident occurs related to security, it can affect the overall image of an organisation. Small enterprises and medium-sized companies have a small budget to invest in securing their data and information. Challenges related to hacking and breaching are very hazardous for the company, and it leads to result in theft of passwords, personal files, emails, confidential information of the company

and many more. In a similar context, a data breach can be defined as an incident that can expose the protected and confidential information that is protected by the company. In addition to this, breaching of data causes various issues, such as theft or loss of password or security number, details related to bank account and credit card numbers, along with personal health information, this type of breach can be intentional or unplanned (Mohammed, Hasan and Awwad, 2020). A data breach can be occurring in any organisation internally or externally. Thus, it is required by any small business organisation to fully enable the software and systems with a complete update, and enabling firewall is also a good way to reduce the risk of breaching attack. In a small organisation, there are a lot of computers which are at the risk of hacking, and each and every system consists of sensitive information about the organisation and personal data of employees which can be further dangerous for the organisation (Lee, Che-Ha and Alwi, 2020).

In the above case, hackers generally attack the small business companies and encrypt the data for taking ransomware from the concerned organisation. The encrypted form of data makes the company give a huge amount of money to the hacker in order to secure and access the data again. It should also be mandatory for every company, whether it is a small scale or large to handle the systems and not allow the employees to take any device to their homes. Moreover, it is also necessary for the organisation to maintain the browser up to date with the help of firewall which protects the computer while surfing the internet (Mohammed, Hasan and Awwad, 2020).

In a similar context, the most common types of security challenges which are faced by small and medium-sized enterprises nowadays include SQL injections, phishing, Denial of Service (DoS), Man in the Middle (MITM) attacks and malware attacks

(Furdek and Natalino, 2020). The data breaching attacks are caused by various types of viruses which can cause a huge loss to the company.

- First one is ransomware attack; in this type of data breaching attack, the hackers encrypt the data of an organisation in order to make money from them to decrypt the data. The companies do not have any chance to overcome this situation; therefore, the company pays the amount required by the hacker. Ransom can come through some malicious websites, emails, and a message from social media, and so on.

- The second type of attack is malware attack which is a quite general attack that consists of viruses and spyware. In addition to this, it can be spread between servers and network on the computers. Most of the malware comes through the passage of emails and social media messages.

- The third challenge is based on the different attempts of data breaching which is called phishing; it is the most common and more affecting form of malware which targets the victim by sending an email which is similar to the form of popular social media sites and bank pages. Along with this, it also comes in a form where the user is asked to download a link, and after downloading the link or filling the form, it injects the virus into computer systems. In the context of form filling, it requests the employees to fill the form which is completely same as the original and after filling the form, employees are not aware of the form being original or fake; hence, the hacker can access and reach the data and also change the passwords of emails and ask for money in order to access the data (Furdek and Natalino, 2020).

In this case, it is mandatory to secure the data in the company by installing antivirus and anti-spyware software in order to save the precious information and data of

clients or the organisation. In addition to this, using Virtual Private Network (VPN) where the surfing is done on the private network is very safe, it can be more useful in saving the data from getting breached. Moreover, encrypting data is also a useful approach in order to safeguard the sensitive data; the encrypting process encrypts the data into a cypher which can only be decrypted by the person who encoded it and by filling the password, the data can be accessed again. Furthermore, in order to prevent from phishing attacks, the small and medium enterprises should provide proper guidance and training to teach the new employees about the policies and guidelines for securing the data and make sure that no one clicks on any unknown link until it is verified by the anti-spyware and antivirus software (Wang *et al*., 2018). There are more serious challenges that are being faced by both small and large enterprises from the beginning of the technological era, wherein the most frequent attack is known as Denial of Service (DoS) attack which is created to shut down the machine or computer network and make the particular website inaccessible. In addition to this, attackers carry out this attack in two ways; the first one is called flooding where hackers or attackers flood the targeted website with a load of traffic which cannot be handled by the server, and it becomes very slow to respond to the visitors of the site. In this duration of flooding, the second process, which is done by the attacker, is to exploit the vulnerabilities which can cause a computer system to crash immediately (Shang *et al*., 2017). In a similar context, DoS attack is identified as irrelevant behaviour of emails, not getting access to the site, disturbing the service of a particular computer system or manipulating the state of information. Another type of DoS attack is known as a smurf attack which is done in the form of automatic responses in personal emails. This type of fake email is sent to everyone in the staff, and if the fake email is clicked by any staff member, their personal email ID comes at the risk of getting hacked. Therefore, it is necessary to provide proper training to

the staff in order to prevent DoS attacks (Shang *et al*., 2017). In relation to the DoS attack, the DDoS attack also perform the same process, but in multiple computers, DDoS attacks are generally made on the global level by taking the help of botnets, a malicious file is distributed by them in order to flood the multiple websites. In this case, DDoS attacks are illegal, and as per the Federal Computer Fraud and Act, the hacker or violator can be sent behind bars for ten years, along with a penalty of almost $50,000 (Shan, Wang and Yan, 2017).

However, the fine and penalty are at its own place, but it can be prevented by applying some security measures in the organisation, such as activating Web Application Firewall (WAF) which is kind of protection with multiple layers between the website and traffic it receives. WAF is costly to buy for the SMEs, but it is the only way to prevent these attacks. The second solution is to consistently analyse the traffic on the website and understand that if an abnormal activity of over trafficking occurs, it is probably a DDoS attack. The third solution is to enable the country blocking the website because working on this type of blocking system is a complicated task for hackers, and it is important to not use any proxy which is not identified (Somani *et al*., 2017).

In the small business, limited budg*et al*ways creates a barrier in protecting the data; cybersecurity comes in the package, which costs plenty of money. In this relation, all the money is wasted if staff lacks in knowledge of cybersecurity and it can be counted as a main security challenge in the SMEs; thus, it is necessary to teach the new staff as well as existing one about the cybersecurity threats which can affect the overall image of the organisation. It is essential for everyone to learn and be secured. In addition to this, bringing one's own device should be restricted in every organisation because it can unleash all the details about the company. If an employee mistakenly leaves his/her laptop or any device which is storing personal data of the company or

information about the client related to medical history, passwords, emails and so on; in this case, it is required by the SMEs to take special care of the devices and ensure that they are connected to VPN. If the employee is not using VPN or using some public Wi-Fi, then it will be quite dangerous for the security of the company, along with this, it is also mandatory to utilise the encrypted channel (Písař and Kupec, 2019).

In order to save the personal data of the company, it is significant to regularly check and update the security tools and software. In this case, it is the responsibility of the Information Technology (IT) manager to protect the small business from security threats (Písař and Kupec, 2019).

Challenges Related to Risk of Malicious Threat from Cybercrime and Non-implementation of ISO 27001:2013 Standard

Risk of malicious threats from cybercrime to SMEs who fail to apply policies related to security

The evolution of the Information and Communication Technology (ICT) has been extensively transforming way of information flow and management not only in larger companies but it is also highly prevalent in the SMEs (Ward, 2015). The people and company's inclination towards using innovations or ICT have been providing advantages to stimulate work efficiency and performance through effective communication and information flow. The extensive benefits of technology advancements or innovations aspire to bring into an existing system or shifts traditional way of information management towards the more interactive way; such as E-commerce, mobile, cloud, social media and apps (Ward, 2015). However, benefits of incorporating innovation bring own issues or problems as well that should

be seriously undertaken to keep vulnerability to a company's stakeholders; including customers, investors, suppliers, employees and sole proprietor or partner as a whole. After the rapidly growing ICT and innovations, cases of information destruction or misuse of information has been increasingly widespread. Information security is the major or serious concern with the ICT adoption to secure from the threat of information hacking or loss to the enterprises' stakeholders. It is because the malicious threats from the cybercrime or information hacking are intentionally undertaken to steal crucial or sensitive data; such as account information and business or personal data for the purpose of misusing for own personal interests (Tufnell, 2014).

The critical issue of cyber-attacks to SMEs due to the poor cybersecurity policies cannot be supposed or considered self-sufficient by the owners of SMEs. The less capital or resources intensive operations of the SMEs cannot be evaded SMEs from cyber-attacks because such SMEs are using information technologies or digital business system without secure system (Shackelford, 2015; Ward, 2015). Around the world, Small and Medium-Sized Enterprises (SMEs) is one of the key contributors to economic growth and have intended to focus on attaining the larger goal of full information security. According to Card (2018), risk of cyber-attacks or crime is not just limited to the larger companies, while SMEs are also at the risk of cybercrime. As per the "General Data Protection Regulation (GDPR), it is important for small-sized to the large-sized businesses to focus on the security of information to ensure the protection of data or systems from the threats of cybercrime (Card, 2018). Similarly, in the info-security magazine, Nice (2017) presented the fact about cyber-attacks to SMEs in the UK. As per the statistics, seven million cybercrime or cyber-attacks hit SMEs in the UK, and its cost to the economy on an annual basis is accounted to £5.3 billion (Nice, 2017). SMEs are unworried about full information security on the

majority that is evident from their poor security policies. In reality, malicious attack from cybercrime is more to the SMEs regardless of the size of operations in comparison to the larger organisations. Cybersecurity is an important and top priority that is only perceived by around 20% of SMEs (Nice, 2017).

In contrast to the larger enterprises, SMEs are more vulnerable to the risk of malicious threats from cybercrime because of their ineffective information security system or security policies that fail to prevent cyber-attacks (Ward, 2015). Lack of technical expertise and encrypted security policies or systems and limited capital or budget are major reasons that SMEs more vulnerable to cyber-attacks (Nice, 2017). It has been generalised that SMEs that fails to apply policies related to security can be a victim of cybercrime that would be the reason for capital loss and closure or shut down at the end.

Information security is defined as an action or practises to prevent access or use of information in the unauthorised or illegal way to ensure no information destruction or misuse for personal use. The unauthorised access to information related to business plans or decisions or information about clients severely poses a risk to stability (Caballero, 2013). The risk of cybercrime is one of the serious concerns or impediments in the way of attaining the larger vision of growth or potential sales and profits. There is a high possibility of being a victim of cybercrime that can be costly in terms of losing potential sales and profits, and the protection of the stakeholders' interests. The importance of understanding eventually risks of cybercrime is indispensable for SMEs because it is an organised crime conducted by skilled hacked on a larger extent. Phishing emails or phishers is the prevalent cybercrime to SMEs that is conducted to access sensitive information from the colleagues or suppliers (Card, 2018).

Trustworthy entitles are approached by hackers to share their sensitive or personal data through a good convincing approach. It is more important for all entitles associated with SMEs to understand different types of cybercrimes and risks of malicious threats. Besides this, anti-virus software usage and strict compliance with all other essential requirements for the information protection act will lead to preventing SMEs from the huge cost or loss due to cybercrime (Card, 2018). The expenses to protect from risks of malicious risks from cybercrime are relatively small for SMEs than a loss as the result of cybercrime (Ward, 2015; Shackelford, 2014). This is the only way to avoid the issue of losing clear or larger vision because good understanding and efficient policies related to the security aids to identify threats from cyber-attaches and potential harm so that immediate actions can be taken along with attaining the larger vision through full security. Overall, efficient information protection system and a good awareness of the cybercrime would have assured meeting goal of full information security to SMEs that eventually helps to flourish at the utmost extent (Shackelford, 2015).

Non implementation of ISO 27001:2013 standard

Information Security Management System (ISMS) defined ISO 27001:2013 standard for application of networking technology in an efficient way because risks prevailing in the external business environment that misuse or destruct important information is all against operational efficiency (Humphreys, 2016). Customer's trust maintenance in terms of information confidentiality or secrecy is the critical issue that against brand positioning or identity. The misuse of the data or illegal access of the information severely worsens the position of an organisation and poses obstruction in the growth and continuity of the operations thereof.

The risk of non-compliance with the standards for information security management induces risk exposure to operational efficiency and sustainable performance. It is because non-compliance has been imposing various issues; such as online fraud, information misuse, data altering and hacking that are all critical concerns in the context of managing customers' trust and confidence. Loss of information is not just capital or financial loss, while it is a loss to goodwill or reputation in the market; thereby non-implementation ISO 27001:2013 standard has been raising challenge in keeping information secured from the unauthorised information users. With the implementation of ISO 27001:2013 standard, it will be extensively possible to less unauthorised access risk or information loss, and thus, it has been analysed that there are more benefits of implementing ISO 27001 than non-implementation (Calder, 2017).

There are various benefits implementing of ISO 27001:2013 standard; such as it lessens the risk to information security or confidentiality. This standard manages security risks through effective internal controls, systematic identification, control or protection from organised hackers or cyber-attacks and keeps compliance with information security (Calder, 2017). Besides this, ISO 27001:2013 standard is being used a proof of efficient security policies or security management, security expertise development and customer confidence or trust that eventually contribute to the robust business growth (Calder, 2013). There is a negative relationship between non-implementation of ISO 27001:2013 and sustainable growth because customers and other business stakeholders are likely interested in continuing and carrying out business with firms that are more secured in terms of the information system management because of capital investment and information confidentiality, as well as integrity (Shojaie, Federrath and Saberi, 2014).

Non-implementation of ISO 27001:2013 standard has been rising to business organisation to ensure customer satisfaction that is business loss or hurdle in the success of capturing opportunities with strong customers' support. Another challenge associated with non-implementation of ISO 27001:2013 standard is a competitive advantage or competitive position along with financial soundness. Secure information system leads to ensure data integrity and data confidentiality along with required information availability to foster performance for the competitive position and inflows of cash and profits due to trust of the customers, investors and shareholders (Calder, 2017). It has been analysed non-implementation of the standard of information management imposes a challenge to flourish business operations with the increased trend of growth. ISO 27001:2013 standard implementation is like a benchmark or certification of efficient business management in relation to the management of information security (Calder 2013). And thus, non-management is indicated to the poor management of information and thus, higher chances of facing issues related to disorganised security policies; such as hacking and cyber-attacks. Moreover, ISO 27001 is an applicable standard at the international level, and thus, non-implementation has been arising challenge to implement effective controls for data integrity, data availability and data confidentiality (Shojaie, Federrath and Saberi, 2014). Overall, it has been generalised that purpose or benefit of ISO 27001:2013 standards are less exposed to the risk from attacks of an intruder. Thus, abidance with the guidelines of ISO 27001 standards; such as procedures and policies in order to mitigate information security risk is significant to keep a competitive edge.

Conclusion

In the 21st century, rapid inclination towards adopting digital business process and ICT has been arousing substantial need for security in terms of efficient security system, technical expertise and in-depth insight of different types of a data breach, data theft and cybercrime. The topic of security in the present era of technological advancements has significant value because of the risk of malicious attacks from the hackers involved in the organised crime. Security influences sustainable performance and growth at the utmost extent because it avoids risks to personal or business data theft and accounts hacking. It can be concluded that knowledge or seriousness towards preventing risks from a data breach, data theft and cyber-attacks is more important to understand by the business owners, employees, supplier and all other key stakeholders, to secure personal and business interests from the hackers.

The inefficient security policies and less concern to the top priority issue of security would make a victim of hackers or organised crime that cause big financial loss to the person or business enterprises as a whole. It can be concluded that good knowledge of security is the key to success in attaining long term goals or vision through operating online or technology-based business transaction within a highly secure environment or system. Based on the discussion and evaluation, it has been generalised that data breach is the critical issue to SMEs to flourish operations privately to attain the vision. In a similar way, data theft is also sustainable performance because of the high possibility of customers' trust being harmed and the possibility of cheating or frauds that against lawful business operations. It has

been concluded that poor security policies and limited or poor security expertise are essential to be improved to sustain a good image in the market.

The timely software update is important to keep strong privacy and security setting, so as to secure data and information from the unauthorised access. In the context of other security concern of risk of malicious threats from cybercrime, it can be concluded that SMEs are more vulnerable to the cybercrime or cyber-attacks regardless of their operations at the small level. SMEs should consider risks from cybercrime as a serious concern with a full security system to keep off from the potential harm. Non-implementation of ISO 27001:2013 standard is also important to be determined by SMEs to deal with an information security risk. Overall, SMEs focuses on the advanced technological environment is not limited to attaining growth, while preventing business and people interests from the security-related risks is also quite substantial to secure from the big losses.

Bibliography

Caballero, A. 2013. *Managing Information Security: Chapter 1. Information Security Essentials for IT Managers: Protecting Mission-Critical Systems*. London: Elsevier Inc. Chapters.

Calder, A. 2013. *Nine Steps to Success: An ISO27001:2013 Implementation Overview*. London: IT Governance Ltd.

Calder, A. 2017. *Nine Steps to Success: an ISO 27001 Implementation Overview.* IT Governance Ltd.

Card, J. 2018. What every SME needs to know about hackers and cyber-security. [Online]. Available at: https://www.telegraph.co.uk/connect/small-business/what-smes-need-to-know-hackers-cyber-security/ [Accessed on: 16 April 2020].

Furdek, M. and Natalino, C. 2020. Machine Learning for Optical Network Security Management. *In Optical Fiber Communication Conference*, pp. 6-8.

Hassan, H. 2020. FACTORS INFLUENCING CLOUD COMPUTING ADOPTION IN SMALL MEDIUM ENTERPRISES. *Journal of Information and Communication Technology* 16(1), pp. 21-22.

Humphreys, E. 2016. *Implementing the ISO/IEC 27001:2013 ISMS Standard*. Artech House.

Lee, C.M.J., Che-Ha, N. and Alwi, S.F.S. 2020. Service customer orientation and social sustainability: The case of small medium enterprises. *Journal of Business Research*, pp. 5-7.

Mohammed, H., Hasan, S.R. and Awwad, F. 2020. Fusion-On-Field Security and Privacy Preservation for IoT Edge Devices: Concurrent Defence Against Multiple Types of Hardware Trojan Attacks. *IEEE Access* 8, pp. 36847-36862.

Nice, S. 2017. Five Reasons Hackers are Targeting SMEs. [Online]. Available at: https://www.infosecurity-magazine.com/opinions/five-reasons-hackers-targeting-smes/ [Accessed on: 16 April 2020].

Písař, P. and Kupec, V. 2019. Innovative controlling and audit–opportunities for SMEs. *Problems and Perspectives in Management* 17(3), pp. 184-185.

Rauch, E., Vickery, A.R., Brown, C.A. and Matt, D.T. 2020. SME Requirements and Guidelines for the Design of Smart and Highly Adaptable Manufacturing Systems. *In Industry 4.0 for SMEs*, pp. 39-41.

Shackelford, S.J. 2014. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. London: Cambridge University Press.

Shan, H., Wang, Q. and Yan, Q. 2017. Very short intermittent ddos attacks in an unsaturated system. *In International Conference on Security and Privacy in Communication Systems,* pp. 45-47.

Shang, G., Zhe, P., Bin, X., Aiqun, H. and Kui, R. 2017. FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks. *In IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pp. 1-6.

Shojaie, B., Federrath, H. and Saberi, I. 2014. Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. I*n 2014 Ninth International Conference on Availability, Reliability and Security*, pp. 259-264.

Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R. 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications,* 107 pp. 30-35.

Tufnell, N. 2014. Big risks for small businesses who ignore data security. [Online]. *BBC News*. Available at: https://www.bbc.com/news/business-27052250 [Accessed on: 16 April 2020].

Wang, P.S., Lai, F., Hsiao, H.C. and Wu, J.L. 2016. Insider collusion attack on privacy-preserving kernel-based data mining systems. *IEEE Access,* 4 pp. 2244-2247.

Ward, M. 2015. Why small firms struggle with cyber security. [Online]. *BBC News*. Available at: https://www.bbc.com/news/technology-31039137 [Accessed on: 16 April 2020].