Dealing with Data Breaches Amidst Changes In Technology

Fuad S. Alharbi *fsa54774@marymount.edu*
Cybersecurity Department
Marymount University
Arlington, 22201, USA

Abstract

The primary aim of this paper is to examine the concept of dealing with data breaches in the age of fast-evolving technology. The paper begins with a definition of a data breach with critical customer information. The research then discusses the major causes of data breaches in Adobe, eBay, Facebook, and Myspace. This paper also details the various types of data breaches including; Ransomware, Denial of service attack, Phishing, Malware or virus, Malicious Insider, Physical theft, and Employee error. With a proper analysis of the data breaches, the research finalizes with a discussion of data security measures that can be used to prevent breaches. These measures are presented in three categories including organizational practices, policies & standards, and organizational practices.

Keywords: Data Breach, Cybersecurity, Technical Practices, Organizational Practices.

1. INTRODUCTION

In the future, it is expected that the industry will be marked with multiple technologies. These technologies will play a crucial role in the improvement of the levels of efficiency that companies exhibit. On the other hand, one of the major weaknesses that will likely arise is a threat to the privacy, integrity, and security of data (Sloane, 2018). Through the use of various technologies such as the internet of things, companies will find it hard to protect their data against breaches (Griffy-Brown, Lazarikos & Chun, 2019). Data breaches will be based on the use of the latest technologies to exploit weaknesses found in the various systems. It is, therefore, recommended that companies must adopt a holistic approach in the development of protective, preventive, and reliable mechanisms of ensuring and guaranteeing information security and reduce the risks of data breaches (Ghosh, Mishra & Mishra, 2019). However, with the current trends, it is expected that more breaches will continue to happen, ranging from the use of phishing, hacking, malware, and also but not limited to ransomware.

Data Breach: A data breach is an incident in which confidential and sensitive, or any protected data is illegally accessed or disclosed without permission. This issue can involve theft or loss of sensitive information such as social security number and password. Data breach can be intentional or accidental and often thrives in environments without proper security measures.

Cybersecurity: Cyber practice entails the practice of creating defense or defending computers, networks and servers and data against malicious attack. This framework allows organizations to cultivate platforms eliminating vulnerable points that can be used by attackers to gain access into the system. As such, the evolvement of technology is opening paths for the introduction of advanced cyber security measures.

Technical Practice: The technical cyber security practices are those that lean towards the technical foundation of an organization. Ideally, the measures comprise

of crafted techniques such as installing firewall, installing malware or adopting a IDS. These technical practices apply to devices and workstations used in business operations in an organization.

2. DATA BREACHES

A data breach is an incident in which confidential and sensitive, or any protected data is illegally accessed or disclosed without permission (Chen & Zhao, 2012). This issue is often associated with crucial information such as credit card numbers and CVV code, social security numbers, medical history, and insurance setup. Besides, data breaches can also target large corporations which aim to obtain customer list, product source code, trade secrets, and payment information. A data breach does not consider the size of the company as both small and established institutions have reported cases of data breaches. Breach of information represents a permanent threat to any organization. Without the proper measures to enhance and quicken the disaster recovery, a business may delay or even ultimately fail to revive its operations.

3. COMPARATIVE ANALYSIS

Over the years, a number of studies have emerged to analyze the issue of data breaches and offer the most suitable solutions to the problem. Marcus, (2018) assessed the proactive solutions that can be used in protecting consumers in case of a data breach. According to the article, creating of proactive solutions can be achieved through setting the minimum security standards, regulation of the use of personal information, introduction of personal identification systems and regulation of social security numbers. Cheng, Liu, & Yao, (2017) also proposed some of the measures that can be used in the prevention of data breaches. This research recommended a number of prevention measures which include; adoption of firewall, installation of intrusion detection programs, data encryption and access control.

Jang-Jaccard & Nepal, (2014) also recognized the existence of security threats that are undermining the performance of data in today's organizations. According to the article, security of data relies on three essential components which include; integrity, confidentiality, and availability. As such, the article recommended a number of measures that can be used in prevention of data breaches which include; data encryption, adoption of virtual private network, cryptography, installation of firewalls and intrusion detection systems. Thakur, Qiu, Gai, & Ali, (2015) further explores in the concept of cyber threat and its impact on data safety. In addition to the discussion of the issue, this article recommends a number of measures that can be used in cultivating data safety. The common measures that can be used to deal with data breaches include; installation of firewalls, adoption antivirus software, and protecting the passwords.

4. MAJOR CASES INVOLVING DATA BREACH

The Adobe case of a data breach in 2013 is considered as one of the biggest incidents of the 21st century. In October 2013, cybercriminals stole login information and gained illegal access to the company's system. This attack lead to the theft of almost 3 million customer credit card information and encrypted passwords for 39 million users (Bell, 2018). Besides, the software developers in the company reported that the hackers gained access to part of the source code to Photoshop editing, which is often used by professional photographers. The company also reported a theft of source code of other three products including; ColdFusion, Acrobat, and ColdFusion Builder. Adobe's spokeswoman reported that the company was not aware of any unusual activity prompting the attack. In 2015, Adobe was instructed to pay a $1.1 million legal fee and also compensated the users following the violation of the Customer Records Act.

eBay also encouraged a massive data breach in 2014 when cyber attackers gain access to 145 million user records (Reuters, 2014). The eCommerce company reported that the hackers were able to access the names, addresses, date of birth and the encrypted passwords of the users. This incident, fortunately, did not reveal any customer credit card information. The cyber attackers targeted the credentials of three company employees which was used to gain illegal access into the network. With the employees' credentials, the hackers had complete access into the network

for 229 days which is was sufficient to compromise the user database (Reuters, 2014). Upon confirming the data breach, the company encouraged the customers to make new and unique passwords. This incident results in huge criticism of the company's approach to store and secure consumer information.

Facebook is another 500 fortune that encountered a data breach in 2018. The attack in the network resulted in the exposure of information of nearly 50 million users (Isaac & Frenkel, 2018). These attackers were able to gain access to the network through the exploitation of features in Facebook code which further provided unauthorized entry into the user accounts and also allowed to gain control of the accounts (Isaac & Frenkel, 2018). Besides, three software flaws were reported to enable access into the user accounts including those of top executives. These software bugs painted a bad image on the company that is known to take pride in engineering. After confirming the data breach, Facebook notified the public that it had taken control of the issues and also notified the law enforcement officials.

Moreover, Myspace also reported a data breach incident in 2013 which resulted in the access of 360 million accounts (Weise, 2016). Cyber attackers gained access to its old platform which resulted in din the compromise of various user information including email addresses, passwords, and usernames. Following the confirmation data breach, the company took the notion to invalidate all passwords belonging to the accounts. The stolen information was put into the dark web for sale and also leaked to LeakedSource (Weise, 2016). Besides, the company responded by monitoring any suspicious activities occurring in the Myspace accounts. Following the dominance of Facebook, Twitter, and Instagram, Myspace still has an active status. Cybersecurity experts reported that users with accounts who do not practice proper password setups are still vulnerable to attack.

5. TYPES OF DATA BREACH

Ransomware refers to a type of data breach that involves a criminal attacker encrypting files and blackmails target organization or victim into paying money in exchange for the decryption key. It is the fastest-growing form of data breaches affecting many organizations. The attackers threaten to destroy critical data if the victim or affected organizations fail to comply with extortion demands. However, the fraudsters do not guarantee to provide a decryption key if the victims decide to pay the ransom. The most form of ransomware delivery system is phishing spam attachments that come to the victim through an email disguising as a file one should trust. However, ones the file is downloaded and opened, the attackers take over the victim's computer, and the blackmail begins. The threat of ransomware is so enormous considering that almost every organization is prone to the attack. In particular, regardless of the network's resilience, the malware is always planted in attachments that sneak past the security firewall unnoticed. Access to computer files is a critical operation in an organization which is indictive that if the attacker takes hold of the files, productivity halts costing the firm millions (Bendovschi, 2015).

A denial of service breach occurs when authorized users cannot access information systems, networks, or devices caused by the actions of malicious cyber threats attackers. The major services affected by the breach may comprise online accounts, emails, or other services that depend on the affected network or computer. The breach works by flooding traffic on the target host until it crashes or the host cannot respond to the attack which prevents legitimate access by authorized users. DoS often cost organizations millions of money or time. The most common techniques of accomplishing Denial of Service breach encompass Smurf Attack and SYN flood. In a Smurf attack, the criminal sends Internet Control Message Protocol broadcast packets to various hosts with spoofed source Internet Protocol address of the target machine. The recipient responds thereby being flooded with responses. On the other hand, a SYN flood happens when an attacker sends requests to connect to the victim's network server but fails to finish the connection through a three-way handshake. The unfinished handshake then leaves the connected port in an unoccupied and unable to receive future requests. The cybercriminal

proceeds to sends the requests until all exposed ports are saturated preventing legitimate users from connecting (Seemma & Sowmiya, 2018).

Phishing is a method of a data breach that attempts to collect personal information of a target victim or organization by using deceptive websites and emails. The attacker uses disguised emails as a weapon to attack. In particular, the aim is to trick the victim into believing that the message is something they need or want, for example, a bank request, or a note from a colleague which persuades the victim to download and open the email attachment. The technique is one of the oldest forms of cyber attacks and takes the form of masquerading into a trusted person or company associated with the victim. It is evident that emails are the most common part of people's lives making them a channel for cybercriminals (Srinivasan, 2015).

Malware as a name given to numerous malicious software programs used by the cyber attacker. Malware attacks include codes designed by the attacker to cause extensive damages to information and systems or gain illegal access to a network or computer system. The data breach is often delivered through a link or file over emails and expects the user to open the file or click on the link to implement the malware. The attacker uses malware to either steal sensitive information from the victim or to demand ransomware. The major malware programs include worms, viruses, trojans, and spyware. A virus is the most common type of malware and is always attach malicious code and wait for an automated process or unsuspecting user to execute the virus. They spread widely and cause massive damage. Spyware on the other hand is designed to spy on the activities of the user. It hides in the background of the computer and gathers information such as using credit card details and password to confidential information (Valuch, Gabris, & Hamulak, 2017).

Also known as insider threat and involves employees that are the cyber attackers or help criminals to accomplish the attack either due to revenge or being blackmailed by the attacker. Some employees do this in attempts to take his revenge especially when they feel unappreciated or have been retrenched. Therefore, the employees try to revenge by jeopardizing the operations of the organization. Others do so to achieve financial gains. Such employees steal data from the company and sell it to the dark web. Organizations are trying to avoid this type of attack by giving employees limited access to the firm's sensitive information. The attacker doesn't have to be a current employee of the firm but can be a former worker, a business partner, a consultant, or a board member. The major types of insider threats comprise the pawns and the turn cloaks. Pawns are a normal employee who is not malicious but makes a mistake opening the door for the actor to exploit or otherwise leads to information loss or compromise. For instance, when a worker mistakenly emails a document containing sensitive information to a wrong person. Conversely a turn cloak is an employee who maliciously and deliberately steals data from the organization (Seemma & Sowmiya, 2018).

It is evident that not all data breaches attribute to digital information. Physical theft is becoming prevalent in many organizations. Attackers can steal items such as paper records and devices that contain sensitive information. This happens when paper information isn't properly disposed of ending up in the wrong hands. For instance, when documents are thrown away without shredding a crook can obtain the information and use it for malicious purposes. Organizations are also encouraged to be careful when disposing of devices such as USB sticks and computers by ensuring that everything is wiped from the equipment. Physical theft can also happen when workers leave records and devices unattended in a plain view (Valuch, Gabris, & Hamulak, 2017).

Employees are the primary security vulnerability for any organization. Therefore, companies are just a click away from system, data, or network damage. Attacks are often as a result of an employee forgetting to follow procedures which then leaks information. For example, when an employee sends bulk emails to many recipients and uses Cc instead of Bcc field thereby sending information to the wrong people. The recipients can then view the information of everyone else who received the message. This can be disastrous when the document contains confidential

information. Moreover, employees can also be responsible for data breaches indirectly by committing mistakes that make it easier for attackers to gain access to private data of the organization. An employee can also erroneously send a wrong document to the intended person which can result in data breaches. Although its human nature, employees need to understand the critical components of information security (Bendovschi, 2015).

6. CYBERSECURITY MEASURES

Management of data breaches involves a combination of various measures which can be categorized into; technical, organizational, policies & standards (Lykou, Anagnostopoulou, & Gritzalis, 2018). This section presents an overview of the cybersecurity measures that can be used to prevent data breaches in an organization. These measures are presented in figure 1 below;

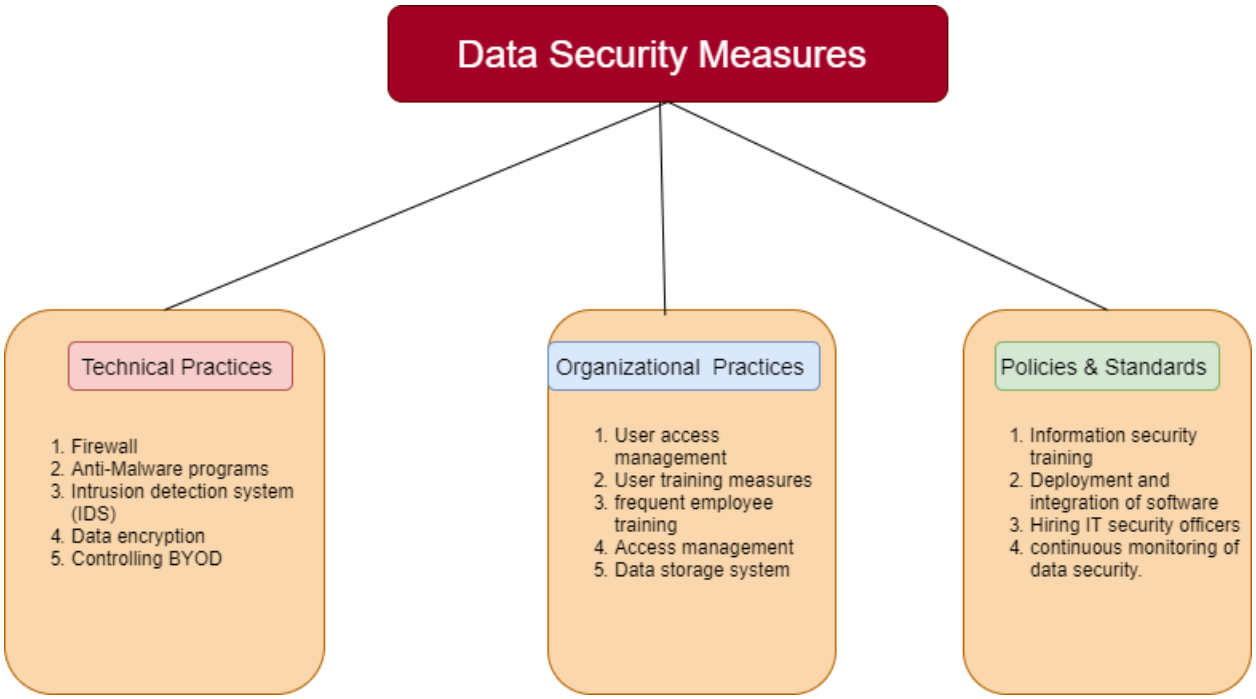

FIGURE 1: Cybersecurity Measures From: (Lykou, Anagnostopoulou, & Gritzalis, 2018).

6.1 Technical Practices

One of the key technical practices that should be implemented by organizations is firewall setup and the network architecture. The border of a business network infrastructure should be protected from unauthorized access. As such, the firewall monitors the flow of traffic hence allowing or preventing access into the network based on the set rules (Cisco, 2020). The installation of anti-malware programs in the organization's system is another technical strategy that can be used to manage data breaches. All computers used to access and store data should have a running anti-malware software that can detect and prevent malware. This strategy ensures the protection of data integrity. Besides, safe data relies on a proper intrusion detection system (IDS). This strategy monitors both the hardware and software systems running over the network (Liao, Lin, Lin, & Tung, 2013). Essentially, it allows an organization to identify any case of illegal attempt to gain access into the system hence raising alerts. With such a strategy, the issue can be escalated and prevented in a timely manner.

Data safety also relies on data encryption. This strategy is often utilized to protect sensitive information transmitted over an open network such as the network. Data encryption prevents any case of eavesdropping during the transmission process. Moreover, strong user authentication is

another measurement that can be used to prevent data breaches. Unique passwords, for example, is a common technique used in creating user authentication hence preventing illegal bypass into sensitive information (Kong, Lei, & Ma, 2018). Also, companies should develop a proper framework for controlling Bring your own device (BYOD). Organizations should set security policies that prevent employees from integrating their personal devices into the organization's systems.

6.2 Policies & Standards

One of the policies that should be set up by a business is the specialized info security training. Organizations should ensure that their employees are up to date with security issues which can be achieved through continuous training. Besides, businesses should enforce the rules used in the deployment and integration of software into the systems. In this case, specific rules should be established to ensure that it covers the installation process of software. Also, companies should set up the standards used in hiring and selecting IT security officers. In this case, the selected officers should have the right skills and aptitudes to deal with data security. Companies should also cultivate a culture of continuous monitoring of data security. Ideally, a company should not wait for an attack to monitor the degree of its data security.

6.3 Organizational Practices

User access management is a crucial component used in the management of data breaches. This practice can be achieved by educating the users on how to ensure a high level of security on their end (Chen & Zhao, 2012). Besides, businesses should adopt proper user training measures. It is not unusual to encounter users who do not know about anti-malware programs that should be installed in the devices. Also, the businesses should introduce frequent employee training on security issues and measures. Companies should also ensure access management before granting access to the systems. This practice ensures that any illegal attempt to gain access to the network. Moreover, companies should introduce proper data storage systems. For example, the systems should have the scalability feature to handle any growth of data over time.

7. CONCLUSION

Data is increasingly becoming intertwined with business operations today. As such, cybercriminals are continuously developing new and updated high tech measures to gain illegal access into the business system; especially those with sensitive and valuable information such as social security number and credit card details. The most common types of data breaches include; ransomware, cybersecurity, denial of service, phishing, malware, insider threats, physical theft, and employee error. As such, the proper measures that can be introduced to deal with breaches comprise technical, polices & standards, and organizational practices. Ideally, businesses should learn to integrate these measures to ensure a maximum level of security in the operations.

8. REFERENCES

[1] Bell, T. (2018). Adobe's CSO talks security, the 2013 breach, and how he sets priorities. *CSO*.

[2] Bendovschi, A. (2015). Cyber-attacks- Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*, 24-31. doi: 10.1016/S2212-5671(15)01077-1

[3] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.*

[4] Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211.*

[5] Cisco . (2020). What Is a Firewall?

[6] Isaac, M., & Frenkel, S. (2018). Facebook Security Breach Exposes Accounts of 50 Million Users. *New York Times* .

[7] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80(5), 973-993.*

[8] Kong, W., Lei, Y., & Ma, J. (2018). Data security and privacy information challenges in cloud computing. *International Journal of Computational Science and Engineering, 16(3), 215-218.*

[9] Liao, H. J., Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36(1), 16-24.*

[10] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve cyber-resilience. *In 2018 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.*

[11] Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ, 68, 555.*

[12] Reuters. (2014). Hackers raid eBay in historic breach, access 145M records. *CNBC*.

[13] Seemma, P., & Sowmiya, M. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128. doi:10.17148/IJARCCE.2018.71127

[14] Srinivasan, S. (2015). Privacy Protection and Data Breaches., (pp. 429-444). Houston. Retrieved from https://pdfs.semanticscholar.org/0675/bbd99274c5410c6c466e851096ff092d88b1.pdf

[15] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 307-311). IEEE.*

[16] Valuch, J., Gabris, T., & Hamulak, O. (2017). Cyber Attacks, Information Attacks, and Postmodern Warfare. *Baltic Journal of Law and Politics, 10*(1), 63-89. doi:10.1515/bjlp-2017-0003

[17] Weise, E. (2016). 360 million Myspace accounts breached. *USA TODAY*.