

uy
by Uu Uu

Submission date: 22-Apr-2020 06:09PM (UTC+0300)

Submission ID: 1304590777

File name: Data_breaches_7pgs.edited_1_1.docx (27.15K)

Word count: 2357

Character count: 12695

DATA BREACHES

by (Name)

Course

Tutor

University

City

Date

Data Breaches

³ A data breach is one of the network and security issues today, where people and organizations are affected. It refers to the intentional or mistakenly releases of confidential data to unauthorized people. The leading forms of data breaches are ransomware, malware, phishing, and denial of service (DoS). The practice has become a significant concern, after the realization that hacking occurs every 39 seconds. Multinational companies and federal departments like the United States Office of Personnel Management, Facebook, and Marriott International, among others, have experienced data breach challenges. Recently, it was noted that the practice had become complicated as the frequency is increasing, making the costs incurred too high. The principal target is the high profile organizations, especially in Europe, the United States, and Australia. The paper analyzes the high profile data breaches recorded recently, factors motivating the practice and statutory bills ⁵ such as Australia's Notifiable Data Breach as well as European Union's General Data Protection Rule in developing reliable ways to curb data hacking.

One of the extraordinary profile figures breaches involved the ZDnet, where an elastic search server breach occurred in January 2019. An online casino team hacked the company, where about 108 million bets were affected (Ribeiro, 2019, p. 149). In turn, the group accessed confidential information like customers' names and home addresses as well as deposits and withdrawals information. Justin Paine, the developer of the server, reported that hacking occurred as the system was left open without a password. The elastic search is a free and reliable engine, which helps companies boost their webs as well as search capabilities. According to ZDNet Company, the time frame on when the server was left open, the number of users affected, and the number of hackers was unknown. The other data breach involved Canva, a graphic design site, where more than 139 million users were impacted in May 2019. According to the report by the Security magazine, the hacking exposed usernames, actual

identifications, emails, passwords, and users' locations, among other confidential information (Ribeiro, 2019, p. 151). Of the number affected, 78 million of the users had linked with their Gmail accounts, making the situation worse.

In January 2019, a MongoDB data hacking involving Chinese job applicants was reported. Cybersecurity experts, Bob Diachenko and Hacken, discovered an 854-gigabyte database, with 202, 730, 434 records on job seekers in China (Ribeiro, 2019, p. 154). The stolen data had the seekers' skills and knowledge, experiences, and other personal details like contacts, email addresses, status, political affiliation, height, and weight, among others. Classifieds Company revealed that the breach was done by a third party that cooperates with companies in collecting data from professional websites. Fortunately, recovery was made seven days after the realization of the mistake. In May, the same year, Diachenko reported another case, involving 275 million records of Indian residents. Here, 275, 265, 298 records were retrieved, giving the details of Indian citizens in a highly PII (Ribeiro, 2019, p. 155). The MongoDB was hosted by the Amazon AWS, where details of names, gender, birth dates, education levels, and professional information were exposed for two weeks.

The other data hacking was recorded in April last year, involving the Facebook App, where two third parties exposed 540 million records (Sloan and Warner, 2019, p. 119). One of the databases affected initiated from the Cultura Colectiva, a Mexican Organization where 146 gigabytes having over 540 million records were exposed. The data presented had users' comments, likes, opinions, and Facebook I.D.s, among others. Additionally, the other third party exposed was 'at the pool' whose information was also posted to the public internet through the Amazon S3 bucket as reported by researchers. It was a data backup, with details on usernames, friends' lists, music, photos, events, and groups, among others. Consequently, in January 2019, a collection data breach case affecting 773 million data records was reported by expert Troy Hunt. The cybersecurity expert found 2, 692,818, 238 rows of data, gotten

from different sources of data breaches entailing thousands of users (Sloan and Warner, 2019, p. 119). The rows had email addresses and passwords, including the updated security aspects by the companies. As a result, the affected companies asked Hunt to gather the files and present on the MEGA cloud service, whereby 12,000 individual files were presented with over 870 GB of data. The expert also located the forums where the stolen data was advertised. Notably, the expert found his details; especially email addresses and passwords that he had used in the past years.

In April, Diachenko and Troia announced a verification data breach, where over 808 million records were hacked. The Mongo D.B.D.B. was accessible by the public, where 150 gigabytes on marketing data was found (Sloan and Warner, 2019, p. 119). The database was owned by a verifications firm, where its email details had leaked. The database also had three other sections, named email records, an email with phone numbers, and one for business leads. As a result, the company took quick actions as the system went offline the same day the expert informed them. Lastly, the American data breach occurred, exposing over 885 million records. Notably, the company is the largest real estate insurance corporation in the country. A journalist and investigator called Brian Krebs reported that the hacking had leaked millions of documents with data on mortgage deals since 2003 (Adlakha et al., 2019, p. 399). Specifically, the confidential data exposed was bank accounts, statements, tax records, social security numbers and transaction receipts, and others. The expert added that the files were left on the web browser, without authentication.

The above data breaches were caused by several factors that should be assessed in controlling the problem. One is the presence of old and unpatched security vulnerabilities. According to reliable studies, 99.9% of the high profile breaches are resulted by common vulnerabilities and exposures (Dolezel and McLeod, 2019, p. 327). The risks are not fixed, giving the hackers an easy time to access sensitive data. Data hacking is also contributed by

human error, which accounts for 52% of the recorded cases (Dolezel and McLeod, 2019, p. 327). Some of the universal human mistakes are the usage of weak passwords, sending data to wrong receivers, sharing passwords with supposed people as well as falling for phishing techniques. Studies show that the human error cause is easy to resolve, as companies need to educate the workers on the fundamental data security aspects. Here, people should understand the problem, methods used by hackers, and ways to ensure the security of their data.

Malware is the other cause of the above data breaches. Years before, it was said to occur on personal machines used in homes and other areas. Today, malware has expanded, attacking the company's systems and exposing information. According to the 2015 research by Verizon DBIR, malware activities occur every second (Sloan and Warner, 2019, p. 119). The malware activities are minor compared to other forms, but the number and variations notable make it a factor to consider. The above study noted that 90% of the malware practices were unique, depending on the organization attacked. Also, the variations make it easy for cybercriminals to hack because their tools are customized based on the targets. Primarily, the criminals make changes from time to time, to ensure the target companies do not recognize the processes. As a result, the variation and complexity of the factor make it significant in describing the causes of data breaches.

Data hacking also occurs due to insider misuse, which refers to where workers use the company systems for personal gains. The concept is different from human error, which entails innocent mistakes that make it easy for hackers. In insider misuse, the people involved are aware of the rules but use the machines for individual interests leading to problems. The 2015 study by Verizon also discussed this factor, claiming that most people engage in the practice for convenience at work or monetary gains. Additionally, the researchers noted that this form is hard to notice, where the people executing the methods are part of the organizations and thus trusted to access. Most of these cases were, therefore, realized after

the employees left the companies indicating that the mess done is significant. Fortunately, the study concluded by giving hope that insider misuse would be reduced by information compartmentalization on the network or the cloud applied. It was said that workers access the lesser the files, the harder it becomes for them to access information that would be abused.

The physical stealing of the tools carrying data is the other cause of information breaches (Romanosky, 2016, p. 123). Some of the tools that give sensitive data are laptops, desktops, tablets, smartphones, hard drives, and servers, among others. The nature of the information stored in the devices determines the likelihood of hacking. For example, the tools having sensitive data are easily stolen than those with general data. Reliable data shows that most of the data breaches in this factor occur around the working area, and only a few happen around the company environment. For example, the criminals would steal phones used by the workers to access customers, more than they would take the desktops used when the workload is more. It is also said that these types of thefts are opportunistic other than planned, making it hard to control. Nevertheless, companies should lower the chances of the information being removed, for example, by having strong passwords. The actions mean that though the devices would be stolen, retrieving sensitive data would be hard.

In helping individuals and companies curb the above causes of data breaches, various legislations have been passed. The Notifiable Data Breaches Scheme (NDB) is one of them. It is based on the 1988 Privacy Act, which was revised in 2017, and the NDB developed (Hopkins and Mooney, 2019, p. 433). The leading role of the scheme is to notify the parties affected when a breach occurs and advises on future prevention ways. According to this body, a data breach takes place where personal information is lost, hacked, or the details provided to the wrong person. In ensuring data security, the NDB accepts all the eligible data breaches assessed via the above criteria. The complaints give the information, after which

investigations are done. Based on the results, the victims are advised, especially on the stated policies that the organizations should observe regarding data security. The NDB also interacts with the community, informing them of the operations done by criminals and ways to curb them. Notably, the legislation has helped curb data breaches, where between February 2018 and December the same year, over 812 data hacking was reported, and the affected companies and people took the necessary preventive actions (Hopkins and Mooney, 2019, p. 433).

The other legislation put in place is ¹the European Union's General Data Protection Rule, which has also helped companies comply with security laws, thus controlling breaches. It was established in 2012 when the European Commission resolved that Europe needed to be cautious in the digital era (Hoofnagle et al., 2019, p. 85). The principal aim of the body was to ensure that companies in the member states in the region and beyond became keen on the data breach problem. One of the leaders said that when trust is built, people gain control of their personal information leading to data protection.

The idea is thus based on people controlling their data, so the companies get to fewer risks while interacting with them. As a result, Europe and other countries would benefit from the digital economy integrated into the market. Under the GDPR, the companies must ensure that the personal data collected is legally protected and the strict conditions given are met. For example, the rights of data owners have to be upheld by implementing strategies that protect them. The regulation has also helped curb data breaches, as the citizens and companies become accountable for their involvement with information.

In conclusion, having analyzed the high profile data breaches recorded recently, factors motivating the practice; it is evident that the data breach problem needs reliable and durable efforts if people and companies are to benefit from the digital economy. Additionally, analyzing the parliamentary bills ⁵such as Australia's Notifiable Data Breach as well as

European Union's General Data Protection Rule in establishing reliable methods to prevent data breaches, it is clear that frequency of this practice has increased, leading to complexity and the need to allocate more money. Normally, the criminals target the high profile companies based on the cases explained, as they have a lot of data that would benefit the criminals financially. The causes are mainly human, where vulnerabilities are not fixed, and the people become less careful, giving the cybercriminals chances to conduct malware and phishing, among other forms. For that reason, the governments have considered the problem and passed bills like the Privacy Act of 1988. The Australian Scheme and European Rules are examples of regulations adopted to help citizens and organizations curb data breaches.

References

- ¹ Adlakha, R., Sharma, S., Rawat, A., and Sharma, K., 2019, February. Cyber Security Goals, Issue's, Categorization & Data Breaches. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (pp. 397-402). IEEE.
- ⁶ Dolezel, D., and McLeod, A., 2019. Managing Security Risk: Modeling the Root Causes of Data Breaches. *The health care manager*, 38(4), pp.322-330.
- ² Hoofnagle, C.J., van der Sloot, B. and Borgesius, F.Z., 2019. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), pp.65-98.
- ² Hopkins, D. and Mooney, L., 2019. Caring about the Notifiable data breach: The human impact on victims. *Governance Directions*, 71(8), p.433.
- ³ Ribeiro, L.E., 2019. High-profile data breaches: Designing the right data protection architecture based on the law, ethics and trust. *Applied Marketing Analytics*, 5(2), pp.146-158.
- ⁷ Romanosky, S., 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), pp.121-135.
- ¹ Sloan, R.H. and Warner, R., 2019. How Much Should We Spend to Protect Privacy: Data Breaches and the Need for Information We Do Not Have. *JL Econ. & Pol'y*, 15, p.119.

ORIGINALITY REPORT

11%

SIMILARITY INDEX

5%

INTERNET SOURCES

4%

PUBLICATIONS

11%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to University Of Tasmania

Student Paper

3%

2

Submitted to University of Derby

Student Paper

2%

3

Submitted to Asia Pacific International College

Student Paper

2%

4

Submitted to University of Maryland, University College

Student Paper

1%

5

www.risklogic.com.au

Internet Source

1%

6

Submitted to Adtalem Global Education

Student Paper

1%

7

Submitted to University of Northumbria at Newcastle

Student Paper

1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off