Vulnerability Cost of Breach Calculator

Research Manual

By

Name: Sarah De Vries

Student ID: C00231717

Project Supervisor: Paul Barry

Date: 13th November 2020

Table of Contents

Introduction

Over the years hacking and other forms of illegally obtaining data has become more frequent and advanced. Even with the increased frequency of attacks cybersecurity still remains low on the budget for many companies and organisations. This will often have catastrophic consequences as they will be incredibly underprepared in the likely event that they become victim to a cyberattack or data breach. A cyberattack will often leave companies, who have filed to prepare themselves, scrambling to resolve the issue resulting in possible millions in revenue, loss in business and a steep drop in their reputation.

This project will focus on increasing awareness of the importance of a strong cyber plan to protect an organisation from cyber criminals. It will examine the types of breaches, some of the legislations surrounding them and some of the data breaches in the last few years that have had a lasting impact on how data is stored.

Historical Perspective

Overview of Data Breaches

The event of a data breach occurs when private and/or confidential information has been accessed either intentionally or accidently.

"Breaches are the result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within" (Sobers, 2020)

The common types of data breaches/attacks are:

- Phishing – This occurs when hackers send messages such as emails that have the appearance of legitimate sources. They will contain links that when activated can steal personal information or perform a malicious action.

- Malware – An umbrella term referring to any type of software that is intentionally designed to cause damage or harm to a device, server or network. These often include:
    - Virus – ILOVEYOU in 2000 costing $15 billion
    - Worm – Stuxnet 2010
    - Trojan Horse – Zeus in 2007 costing $3 billion

- Ransomware – A type of malware that encrypts the files on a computer demanding a ransom to restore access to the victim's data. The victim will receive a message informing them of what has occurred stating they need to pay a fee for a decryption key. An infamous example of the extent of damage that ransomware is WannaCry from 2017. It was introduced in phishing emails and over 200,000 people were affected. Hospitals and large companies, such as FedEx and Nissan were also breached. The total cost was $4 billion. *(Gatefy, 2021)*

- Denial of Service – A DoS attacks has the purpose of making a machine or network inaccessible to its legitimate users. This is accomplished when the target network is flooded with traffic often causing it to crash.

Even though data breaches appear to be occurring more often with the rise of technology such as cloud computing, they actually existed as long as companies have kept confidential data and private records. Data breaches that have been disclosed to the public became more prevalent in the 1980s with awareness for data breaches growing in early 2000.

2005 was an eventful year in terms of data breaches, with two of the main events that occurred being:

- **Over 1 million records compromised:** This occurred when DSW Show Warehouse was attacked by hackers and had 1.4 million credit cards and numbers stolen.

- **First college to experience a data breach:** The College attacked was George Mason University which had 32,000 student and staff names, pictures and social security numbers breached.

Along with these two 2005 events, CardSystems, a payment card processor, was victim to an incident where hackers exposed 40 million credit card accounts.

(LifeLock, 2018)

Statistics

Below is a collection of statistics and facts regarding data breaches.

1. **Hacking attack every 39 seconds:** A study was carried out by the University of Maryland where a group of computers were analyzed. It was noted that the computers were attacked roughly 2,244 times a day. It was also discovered, during the study that the majority of the attacks against the computers came from hackers using “dictionary scripts”. *(O'Driscoll, 2020)*

2. **Attacks are not discovered quickly:** 2019 saw many attacks go unnoticed for months at a time. American Medical Collection Agency, for example, was victim to a breach starting in August 2018 which was only discovered near the end of March of the following year. Ponemon’s Cost of a Data Breach Report estimates the time it takes to discover and fix a breach takes around 279 days. *(Fasulo, 2019)*

3. **Where the attack comes from:** An interesting statistic to note is that 1 out of 4 breaches were due to inside jobs. These can be due to espionage, financial gain and even honest mistakes. With data breaches as a whole, 73% were performed by an outside party, 28% from the inside, 2% by partners and the remaining 2% from multiple parties. *(Bera, 2020)*

Other Statistics

- “The Creeper”, was the first computer virus and it was discovered in early 1970
- AOL was the first victim of phishing attacks in 1996
- During the first half of 2018, 56% of data breaches came from social media platforms

(Sobers, 2020)

- In 2019, the most data breaches were experience by the business sector.
- Out of the data breaches that occur, 27% of them involve phishing emails.
  (Bera, 2020)

5 Major Data Breaches

Yahoo

Year:	2013
Affected:	3 billion accounts
Cost paid:	$117.5 million

In August of 2013, Yahoo has hit with cosmic data breach where it was initially thought that hackers had cause 1 billion accounts to become compromised. This estimation was later raised up to 3 billion in 2017, meaning all their user accounts had been compromised. When the investigation had gone under way it was revealed that credentials such as payment and bank information had not been stolen. However it was also discovered that users' passwords had been stored in plain text and security questions and answers had been compromised.

The report of the breach had not come at a good time for Yahoo as it occurred while negotiations were taking place with Verizon to buy them over in 2016. With the reported breach made apparent, before the true numbers were discovered, all users were forced to change their current passwords and resubmit any security questions and answers which weren't initially encrypted. *(Tunggal, 2020)*

Jeremiah Grossman was an information security officer for Yahoo who went on to become the chief of security strategy at SentinelOne. When talking about the incident *said "They are as big as it gets, [...] Maybe Google or maybe Facebook, but the next mega-breach is not going to be orders of magnitude bigger*." *(Newman, 2017)*

Some criticize how Yahoo handled the incident with the investigation taking nearly four years to complete added to the three years it took to discover and report the breach. This is on top of the separate breach that occurred in 2014 and was not reported for another two years where another 500 million accounts were affected.

The Yahoo data breach is still one of the largest to occur in history

First American Financial Corp

Year: 2019
Affected: 885 million people
Cost: over $5 million

Founded in 2008, First American Financial Corp provides insurance and settlement services based in California. The large company employs over 18,000 and in 2017 had reported assets that exceeded $9 billion.

It was revealed that in May of 2019, First American Financial Corp leaked 885 million sensitive records. It was noted that the records dated back over a decade and included information containing social security numbers, mortgage paperwork, banking details and other. It was found that a U.S financial service company had these details accessible to the public on their server.

The online files were discovered by Ben Shoval, who is a real estate developer, who then informed Brian Krebs, a security reporter. Krebs the n contacted the owner of the server before reporting the incident.

A spokesperson for the company stated that the reason for the unauthorised access of private data was due to a design defect in a production application. It was also reported that it was possible to access the confidential information without any authentication.

It was noted that Shoval said that the millions of documents dating back as early as 2003 possessed *"all kinds of documents from both the buyer and seller, including Social Security numbers, drivers licenses, account statements, and even internal corporate documents if you're a small business." (Cameron, 2019)*

Marriott International

Date: November 2018
Affected: 500 million guests
Cost: $28 million

Marriott International made the announcement, that the Starwood reservation system had been breached and up to 500 million guests' personal data had been stolen. This data included names addresses, phone numbers, email addresses, encrypted credit card details and more. With the data that was stolen, a small group of guests also had their travel history and passport numbers stolen. It was noted that the breach began as early as 2014 and comes seconds to the Yahoo breach that occurred in 2013 where the entire user base was affected. *(Nicole Perlroth, 2018)*

Due to the value of the data stolen and the large amount of it, there were concerns raised that Marriott may have been target of hackers looking to gain information on the movements of high profiles like diplomats, spies, military officials and business executives.

This data breach occurred around the same time as a number of other breaches against American health insurers and government agencies such as the United States Office of Personnel Management. Many thought these attacks were to put together a large collection of information on people who were later to be espionage targets.

During a news release Arne M. Sorenson, a chief executive for Marriott, stated that *"We deeply regret this incident happened. We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward." (Taylor Telford, 2018)*

Friend Finder Networks

Date: October 2016
Affected: 412.2 million accounts

According to a report from LeakedSourse, a website for breach notifications, a hacking incident against FriendFinder Networks, an adult dating and entertainment company, exposed data from 412 million accounts. The data went back 20 years and contained credentials such as username, passwords, emails and date of last visit.

The breach didn't only affect the main site but also a couple other owned sites including Cams.com and Penthouse.com. There was a possibility that, within the amount of data breached, 15 million email addresses of deleted accounts were also breached. The new owners of Penthouse.com stated that they were aware of the apparent breach and that they were *"waiting on FriendFinder to give us a detailed account of the scope of the breach and their remedial actions in regard to our data." (Peterson, 2016)*

When approached by The Washington Post, FriendFinder Networks did not attempt to confirm whether or not this was true. However they did making a statement saying that they have *"received a number of reports regarding potential security vulnerabilities from a variety of sources [...]. Immediately upon learning this information, we took several steps to review the situation and bring in the right external partners to support our investigation." (Peterson, 2016)*

FriendFinder Networks had experienced a separate breach back in May 2015 that affected 3.5 million user accounts.

Adobe

Date: October 2013
Affected: 153 million user records
Cost: $2.1 million

At the beginning of October, a security blogger named Brian Krebs revealed that Adobe had reported a breach. This breach consisted of hackers stealing close to 3 million encrypted customer credit card records. This also included login data for a number of user accounts.

Upon viewing the monumental amount of illegally obtained account data, KrebsOnSecurity stipulated that in addition to the encrypted credit card records, that *"tens of millions of user accounts across various Adobe online properties may have been compromised in the break-in." (Krebs, 2013)* Since many of the directories being protected by passwords, this made it complicated to try and completely examine the majority of the files on the hackers' server. Adobe was also unwilling to provide an estimate to the true amount of those potentially impacted.

Further into October a massive 3.8GB file labelled as "users.tar.gz" was posted on AnonNews.org containing over 150 million usernames and hashed password pairs that were taken from Adobe.

According to Heather Edell, a spokesperson for Adobe, the company had recently gone through the process of contacting all active users whose user IDs with valid encrypted password information was stolen because of the breach. Any users contacted were urged to reset their passwords.

Later in August 2015, an agreement was put in place for Adobe to pay a total of $1.1 million in legal fees. They also had to pay an unspecified amount of money to users, which was to settle any claims of Customer Records Act violations along with unfair business practices. By November 2016, it was revealed that the amount Adobe had to pay out to customers was $1 million. *(Swinhoe, 2021)*

Data Breaches in 2020

Twitter

Date: July
Affected: 130 000 targeted accounts
Cost: to be determined

On July 15th of this year, Twitter was hit with an impressive attack involving bitcoin where hackers gained control of verified accounts, including Barack Obama, Bill Gates, Elon Musk and more, sending out tweets with *"I'm giving back to the community. All bitcoin sent to the address below will be sent back doubled! If you send $1000, I will send back $2000. Only doing this for 30 minutes." (Keepnet, 2020)* This message managed to reach over 3 million people which in turn resulted in recovery of stolen donation of £86,800 within a matter of hours.

In relation to this attack cybersecurity experts claimed "*the social engineering featured in this scam demonstrates that the attackers targeted Twitter employees with access to internal tools and preyed on the trust associated with verified accounts and the attraction of doubling your money." (Kelly, 2020)*

During the attack, the team at Twitter weren't sure of effective measure they should take as shutting off the service completely may not have been possible. Later on the team made the executive decision to block any accounts that were verified from tweeting from those accounts.

While this appeared to work this created many other issues. Since verified accounts were unable to send tweets this created an "information bottleneck" *(Thompson & Barrett, 2020).* The National Weather Service were unable to broadcast a tornado advisory and other media companies were unable to inform users of the breach occurring. This left the official Twitter Support account as the only reliable source of information.

Twitter will more than likely have to deal with legal consequences with the EU's General Data Protection Regulation (GDPR) stating that platforms like Twitter should already have an appropriate level of security in place *(Tidy, 2020).*

Marriott International

Date: February-March
Affected: 5.2 million guests
Cost: $123 million

After the breach that occurred in 2018, Marriott experienced another data breach affecting the personal details of 5.2 million guests.
The breach was discovered near the end of February and goes back to the middle of January earlier in the year. Marriott stated that during late February, it had realised that an un-named hotel chain's network had been compromised. The hackers had obtained two employees' login credentials and may have gotten access to guests' details. Details stolen include names, phone numbers, birthdates, language preferences and loyalty account numbers.

During the investigation, Marriott made a statement saying that *"While our investigation is continuing, we currently have no reason to assume that the details involved included passwords or PINs for Marriott Bonvoy account, payment card details, passport information, national IDs or driver's license numbers." (lrmax, 2020)* Marriott also stated that any affected guests had been contacted. Many view this as carelessness considering that Marriott had also experienced a separate breach earlier in 2018.

Zoom

Date: April
Affected: 500,000

In recent times Zoom has become a popular app for both virtual meetings and cybercriminals. During the first week of April this year, users were shocked to hear the news that 500,000 stolen passwords had been put up for sale on the dark web and hacker forums. Some of the account credentials were been sold for less than a US cent while some where been given away for free.

These credentials are gathered together and hackers then use them to attempt to login to Zoom. The successful attempts are then put together and sold onto other cyber criminals. It was also discovered that personal URLs, email addresses and HotKeys were available too.

Cyble, a cybersecurity intelligence firm, stated that from the beginning of April 2020 "*they began to see free Zoom accounts being posted on hacker forums to gain an increased reputation in the hacker community." (Abrams, 2020)*

Upon seeing the accounts for sale on the forum, Cyble decided to buy accounts in bulk with the intent to inform the users of the current data breach. Cyble were successful in this venture, been able to purchase 530,000 credentials with the price at $0.0020 per account.

Magellan Health

Date: April
Affected: 365,000

During April of 2020, Magellan Health, the Fortune 500 Company, discovered that they had been victim to a sophisticated social engineering attack. It took a few months to come up with a figure of affected victims, which is now around 1.7 million. These victims include both external companies and internal staff. Magellan Health had also been victim to a previous data breach, a phishing attack, a year before.

During the investigation, it was concluded that the hackers installed that malware with the intent to gain employee credentials so that they would be able to have full access to the server. During this data breach, patient data was also affected which included health insurance account information and treatment information.

"The attack was contained to a single corporate server, which compromised the data of current employees and a trove of sensitive patient data, from Social Security numbers and W-2 information, to taxpayer identification and employee ID numbers." (Davis, 2020)

During the time period of the report it is not yet clear the true number of clients or affiliates that have been affected. The number is currently at 365,000 with this been the third largest healthcare data breach this year.

EasyJet

Date: May
Affected: 9 million
Cost: to be determined

During this year, it was revealed that EasyJet was victim to a highly sophisticated cyberattack where personal information of 9 million customers was compromised. Of these 9 million, over 2000 had their credit card details stolen while it appears that on passport details had been accessed. There was priority contacting those whose credit card details were stolen while the remaining were contacted by the end of the month.

There weren't any immediate details released on how the breach occurred but EasyJet stated that they had *"closed off this unauthorised access and reported the incident to the National Cyber Security Centre and the Information Commissioner's Office (ICO), the data regulator." (Jolly, 2020)*

This breach may result in EasyJet paying a large fine during a financial stressful time for many businesses due to the pandemic. During 2019, British Airways was hit with a fine of £183 million due to a breach where 500,000 customers' personal information was stolen.

Johan Lundgren, the chief executive for EasyJet, made the following statement:

"We would like to apologise to those customers who have been affected by this incident. Since we became aware of the incident, it has become clear that owing to Covid-19 there is heightened concern about personal data being used for online scams.

"As a result, and on the recommendation of the ICO, we are contacting those customers whose travel information was accessed and we are advising them to be extra vigilant, particularly if they receive unsolicited communications." *(Jolly, 2020)*

Legislations

General Data Protection Regulation

The General Data Protection Regulation, belonging to the EU, is made up of rules outlining the way in which companies are to process data. It came into force across the EU on May 25th 2018. The purpose of GDPR is outline responsibilities for organizations to ensure:

- Privacy and protection of personal data
- Provide rights to who the data belongs
- Assign power to regulators to ensure organisations are held accountable for failing to comply with the requirements

Within the General Data Protection Regulation, is Article 5 outlining 7 key principles which make up the core of the data protection regime. These principles have influence, directly and indirectly, over the other rules and obligations.

Obligations

Following the guidelines of the GDPR and Data Protection Acts 1988-2018, when collecting data there is a legal responsibility that:

1. It was obtained lawfully, fairly and with complete transparency
2. Use is limited to the purpose
3. Only the relevant and accurate data is obtained and not excessive
4. The data is to be kept accurate
5. The data is only stored for as long as is necessary
6. The data is processed in a way that will ensure security of the data against unauthorised/unlawful processing. This also includes protection against damage, loss or destruction.

(Commission)

Data Subjects' Rights

Alongside the seven principles, a data subject also has the following rights under both GDPR and the Data Protection Act 2018.

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to object

- The right to data portability

GDPR and the Data Protection Act 2018

Along with the GDPR been implemented in May 2018, a new Data Protection Act was also put in place with the purpose of being a supplement to the General Data Protection Regulation. This completed certain sections of the Regulation that, in most cases, are simply left to individual member stated to implement, interpret and apply the provisions.

Data subjects, under the General Data Protection Regulation, have the full right to file a complaint with the Data Protection Commission if they believe that any processing of their personal data violates the Regulation.

Both the General Data Protection Regulation and the Data Protection Act 2018 are equally supported by a regime with significantly higher penalties compared to the Data Protection Act 1998 and the Data Protection Act 2003. On top of that, there are also fines that can go up to €20 million or 4% of the global annual turnover.

Breach Notification

Since the General Data Protection Regulation was put in place it required all organisations are required to report and data breaches to the relevant authority. This must be done within 72 hours of the breach been discovered. In the event that the breach is a high risk to the individuals affected in the breach, the compromised organisations much inform those individuals immediately.

Risk Rating

In order to determine the level of seriousness of the breach for the individual, the impact of said data been exposed for the individual must be considered. Important factors that must be considered are:

- How the breach occurred
- What type of data is exposed
- Are there any mitigating factors in place
- Whether the personal data of a vulnerable individual was exposed

The risk categories are grouped as:

- **Low**: The breach that has occurred is either not likely to impact the individuals or poses minimal impact
- **Medium**: The breach will possibly have an impact which is unlikely to become substantial
- **High**: The breach that has occurred will possibly have a considerable impact on said individual
- **Severe**: The breach is likely to pose a critical, dangerous or extensive impact on the individual in question *(Commission, Breach Notification)*

Prior Work in this Area

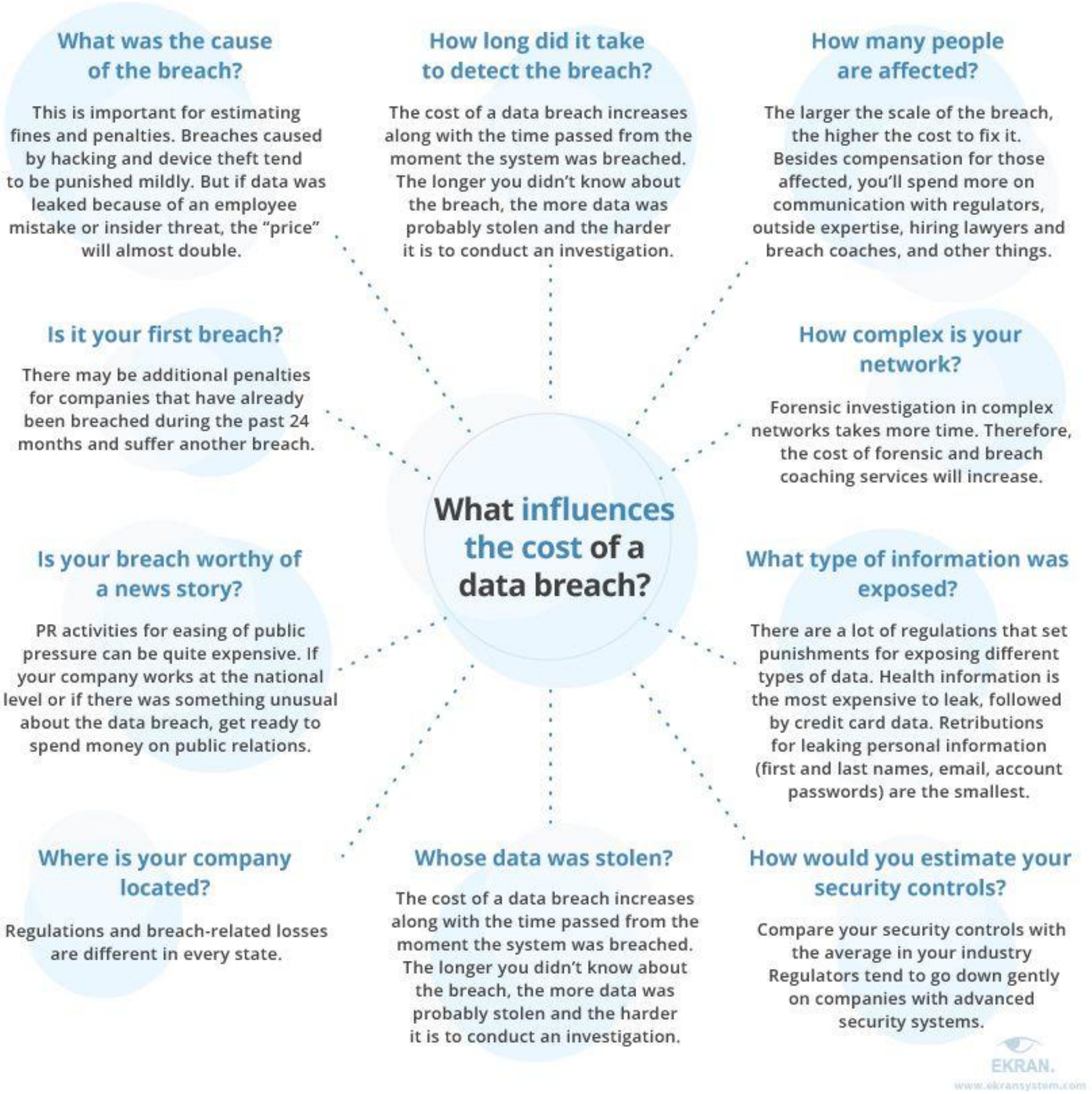
Calculating Data Breaches

In relation to the cost of a data breach incident, there are a few major components that are involved:

- The direct cost – This is the expense that occurs when dealing with a newly detected breach. Factors that are included are any fines, compensation for customers, forensic and investigation etc.
- The indirect cost – This refers to time and any other resources it takes to recover from a data breach such as issuing out new account credentials.
- The lost opportunity cost – Failed or lost business opportunities resulting from negative effects of a data breach. Customers can lose faith in a company in the event of a breach which will result in possible losses.

Location can be a major factor in the calculating costs, for example in 2017the average cost of a data breach in the United States was $7.91 million while in Brazil it was lower at $1.24 million.

(Ekran, 2018)



What influences the cost of a data breach?

What was the cause of the breach?

This is important for estimating fines and penalties. Breaches caused by hacking and device theft tend to be punished mildly. But if data was leaked because of an employee mistake or insider threat, the "price" will almost double.

How long did it take to detect the breach?

The cost of a data breach increases along with the time passed from the moment the system was breached. The longer you didn't know about the breach, the more data was probably stolen and the harder it is to conduct an investigation.

How many people are affected?

The larger the scale of the breach, the higher the cost to fix it. Besides compensation for those affected, you'll spend more on communication with regulators, outside expertise, hiring lawyers and breach coaches, and other things.

Is it your first breach?

There may be additional penalties for companies that have already been breached during the past 24 months and suffer another breach.

How complex is your network?

Forensic investigation in complex networks takes more time. Therefore, the cost of forensic and breach coaching services will increase.

Is your breach worthy of a news story?

PR activities for easing of public pressure can be quite expensive. If your company works at the national level or if there was something unusual about the data breach, get ready to spend money on public relations.

What type of information was exposed?

There are a lot of regulations that set punishments for exposing different types of data. Health information is the most expensive to leak, followed by credit card data. Retributions for leaking personal information (first and last names, email, account passwords) are the smallest.

Where is your company located?

Regulations and breach-related losses are different in every state.

Whose data was stolen?

The cost of a data breach increases along with the time passed from the moment the system was breached. The longer you didn't know about the breach, the more data was probably stolen and the harder it is to conduct an investigation.

How would you estimate your security controls?

Compare your security controls with the average in your industry Regulators tend to go down gently on companies with advanced security systems.

Figure 1.1 (Ekran, 2018)

As shown in Figure 1.1, there are many factors that will influence the cost of a data breach.

How the breach occurred in the first place will have a big influence on the cost to the company. If it was a mistake made by an employee or an inside threat would result in higher fines/penalties then if the breach was caused by hacking or the theft of a device used. Similarly, the penalties for a company will be steeper if they have been breached previously in the last 2 years.

Another influence is time. The less time it takes to detect a breach, the smaller the penalties. This comes from the idea that the longer amount of time that the breach is occurring the more data and personal information that can be stolen, sold etc. The type of information is also important with health information been the most expensive with credit card details coming in after. Along with those factors, the amount of people that were affected is also considered.

The Ponemon Institute

Founded in 2002 by Dr. Larry Ponemon and Susan Jayson, Ponemon Institute has been dedicated to: “Independent research and education that advances the responsible use of information and privacy management practices within business and government.

“Our mission is to conduct high quality, empirical studies on critical issues affecting the security of information assets and the IT infrastructure.” *(Institute)*

Verizon

Formed in 2000, Verizon is one of the world’s leading providers of technology, information and more.

Taken from the IBM Ponemon “Cost of Breach” 2019 report, it is calculated that in the UK the average cost of a data breach incident is $4.88 million. SonicWall President and CEO Bill Connor commented on the topic stating that *“UK organisations continue to struggle to track the evolving patterns of cyberattacks — the shift to malware cocktails and evolving threat vectors — which makes it extremely difficult for them to defend themselves.” (Rathod, 2019)*

Bibliography

Abrams, L. (2020, April 13). *Over 500,000 Zoom accounts sold on hacker forums, the dark web*. Retrieved November 12, 2020, from BleepingComputer: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

Bera, A. (2020, November 7). *30+ Horrific Data Breach Statistics & The Biggest Breaches*. Retrieved November 19, 2020, from Safe At Last: https://safeatlast.co/blog/data-breach-statistics/#gref

Cameron, D. (2019, May 24). *885 Million Records Exposed Online: Bank Transactions, Social Security Numbers, and More*. Retrieved November 5, 2020, from Gizmodo: https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

Commission, D. P. (n.d.). *Breach Notification*. Retrieved November 10, 2020, from Data Protection: https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification#:~:text=From%2025%20May%202018%2C%20the,becoming%20aware%20of%20the%20breach.

Commission, D. P. (n.d.). *Principles of Data Protection*. Retrieved November 6, 2020, from Data Protection Commission: https://www.dataprotection.ie/en/individuals/principles-data-protection

Davis, J. (2020, July 7). *Magellan Health Data Breach Victim Tally Reaches 365K Patients*. Retrieved November 12, 2020, from Health IT Security: https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients

Ekran. (2018, December 18). *How to Calculate the Cost of a Data Breach*. Retrieved November 6, 2020, from Ekran System: https://www.ekransystem.com/en/blog/cost-of-a-data-breach

Fasulo, P. (2019, December 9). *5 Data Breach Statistics and Trends to Look Out for in 2020*. Retrieved November 19, 2020, from Security Scorecard: https://securityscorecard.com/blog/5-data-breach-statistics-and-trends-to-look-out-for-in-2020#:~:text=1.,same%20time%20period%20in%202018.

Gatefy. (2021, March 18). *11 real and famous cases of malware attacks*. Retrieved April 28, 2021, from Gatefy: https://gatefy.com/blog/real-and-famous-cases-malware-attacks/

Institute, P. (n.d.). *Why We Are Unique*. Retrieved November 20, 2020, from Ponemon: https://www.ponemon.org/about/why-we-are-unique.html

Jolly, J. (2020, May 19). *EasyJet reveals cyber-attack exposed 9m customers' details*. Retrieved November 20, 2020, from The Guardian:

https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card

Keepnet. (2020). *The Biggest Data Breaches in the first half of 2020*. Retrieved November 6, 2020, from Keepnet Labs: https://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020/

Kelly, C. (2020, September 13). *We reveal the biggest data breaches of 2020*. Retrieved November 6, 2020, from CommsMEA: https://www.commsmea.com/business/trends/22392-we-reveal-the-biggest-data-breaches-of-2020

Krebs, B. (2013, October 29). *Adobe Breach Impacted At Least 38 Million Users*. Retrieved November 10, 2020, from Krebs on Security: https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/comment-page-2/#:~:text=In%20a%20breach%20first%20announced,number%20of%20Adobe%20user%20accounts.&text=gz%E2%80%9D%20that%20appears%20to%20include,password%20pairs%20take

LifeLock. (2018, January 12). *A Brief History of Data Breaches*. Retrieved November 13, 2020, from LifeLock: https://www.lifelock.com/learn-data-breaches-history-of-data-breaches.html

lrmax. (2020, April 13). *Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen*. Retrieved November 12, 2020, from Security Boulevard: https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/

Newman, L. H. (2017, March 10). *Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts*. Retrieved November 5, 2020, from Wired: https://www.wired.com/story/yahoo-breach-three-billion-accounts/

Nicole Perlroth, A. T. (2018, November 30). *Marriott Hacking Exposes Data of Up to 500 Million Guests*. Retrieved November 11, 2020, from The New York Times: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

O'Driscoll, A. (2020, July 4). *30+ data breach statistics and facts*. Retrieved November 19, 2020, from Comparitech: https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/

Peterson, A. (2016, November 16). *Adult FriendFinder hit with one of the biggest data breaches ever, report says*. Retrieved November 12, 2020, from The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/

Rathod, L. (2019, August 13). *Cost of a Data Breach: Ponemon Institute Report*. Retrieved November 20, 2020, from Diligent: https://diligent.com/en-gb/blog/cost-of-a-data-breach-ponemon-institute-report/

Sobers, R. (2020, September 24). *107 Must-Know Data Breach Statistics for 2020*. Retrieved November 13, 2020, from Varonis: https://www.varonis.com/blog/data-breach-statistics/

Swinhoe, D. (2021, January 8). *The 15 biggest data breaches of the 21st century*. Retrieved April 26, 2021, from CSO Online: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Taylor Telford, C. T. (2018, November 30). *Marriott discloses massive data breach affecting up to 500 million guests*. Retrieved November 11, 2020, from Washington Post: https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/

Thompson, N., & Barrett, B. (2020, September 24). *How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One*. Retrieved April 26, 2021, from Wired: https://www.wired.com/story/inside-twitter-hack-election-plan/

Tidy, J. (2020, July 16). *Twitter hack: What went wrong and why it matters*. Retrieved April 26, 2021, from BBC: https://www.bbc.com/news/technology-53428304

Tunggal, A. T. (2020, October 2). *The 36 Biggest Data Breaches [Updated for 2020]*. Retrieved November 5, 2020, from UpGuard: https://www.upguard.com/blog/biggest-data-breaches