Assignment One: Google Case Study

Ma'alona Mafaufau - 1284380

Computing, Electrical and Applied Technology, Unitec Institute of Technology

HTCS6701: Information System Security

Conan Bradley

May 9, 2021

Contents

Executive Summary

This report examines a scenario involving a phishing attack on a Google employee that led to a data breach exposing 1.5 billion usernames and passwords and a resulting ransom. Specifically, we explore the legal and ethical factors surrounding various considerations faced by not only Google, but the employees involved in the mitigation of the breach, such as the Google CISO, the designated penetration testers, as well as the employee who fell victim to the phishing attack. Various legal documents have been developed globally in recent times, and an analysis into these documents is performed with the scenario in mind. Finally, we provide advice on whether the ransomware should be paid to the attackers, backed by research seen abroad.

Keywords: Phishing, GDPR, CCPA, NZ Privacy Act 2020, Data breach

Introduction

We briefly introduce the scenario where a data breach of 1.5 billion usernames and passwords has occurred due to a phishing attack on a Google employee. The CISO of Google has informed us to perform a penetration test, however has voiced concerns around the legal implications and risks surrounding the test. Furthermore, a ransom of $1 billion has been requested by the attackers.

Section 1

Question 1

To analyse a decision surrounding data breach disclosure outlined in the assignment scenario, we consider both national and international law, as well as an exploration of ethical factors regarding a course of action following the breach. As Google collects, analyses, and stores the personal data of users across the globe (Vanderbilt University & Schmidt, 2018), including those in the European Union (EU) (EDPB, 2020), we begin by considering the legal ramifications outlined in the General Data Protection Regulation (GDPR).

GDPR

GDPR Data Breach Notification Requirements: The GDPR came into effect on May 25, 2018 (*GDPR – Official Legal Text*, 2019) and so must be considered in our analysis. We examine the GDPR as it is assumed that of the 1.5 billion usernames and passwords breached, a proportion of those belong to residents of the EU, and are thus protected under the GDPR (*GDPR – Official Legal Text*, 2019, "Territorial scope" section). In particular, Chapter 4, Article 33 requires that Google needs to notify the relevant authorities in the event of a notifiable personal data breach as soon as practically possible while being within a time frame of 72 hours (*GDPR – Official Legal Text*, 2019, Chapter 4, Art. 33(1)). Broadly, any adverse effects to the confidentiality, integrity or availability of an EU citizen's data due to a data breach constitutes a 'personal data breach' (Information Commissioner's Office, n.d., "What is a personal data breach?" section) and must be reported if such an event is likely to "result in a risk to the rights and freedoms of natural persons" (*GDPR – Official Legal Text*, 2019, Chapter 4, Art. 33(1)).

GDPR Data Breach Fines: Failing to notify a reportable breach to the relevant authorities within the time frame specified, the GDPR outlines that because of unfulfilled

obligations (*GDPR – Official Legal Text*, 2019, Chapter 4, Articles 24-39), the organisation is subject to fines. We outline the details of these fines in Section 1, Question 2 which analyses the penalties for non-disclosure.

California Consumer Privacy Act (CCPA)

Under the assignment case study scenario and similar to GDPR considerations, it is also assumed that a proportion of exposed usernames and passwords belong to citizens from California. Consequently, we must consider the CCPA as it outlines data protection laws regarding this particular American cohort.

CCPA Data Breach Notification Requirements: The CCPA states that if after 30 days, an organisation has failed to "cure" a violation such as a notifiable data breach containing personal information, that organization is subject to fines (*Bill Text - SB-1121 California Consumer Privacy Act of 2018.*, 2018, Chapter 735, Section 1798.155(b)). The CCPA also outlines specifically that the combination of a username and password, not unlike the data exposed in the Google data breach, is included in the definition of 'personal information' (*Law Section*, n.d.).

CCPA Data Breach Fines: Similar to the fine structure of the GDPR, the CCPA fines have a two-tiered system, which are outlined in Section 1, Question 2 of this report.

NZ Privacy Act 2020

We also assume that NZ citizen data has been included in the data breach. Therefore, Google is subject to the consequences outlined in the NZ Privacy Act 2020.

NZ Privacy Act 2020 Data Breach Notification Requirements: Part 6, Section 114 states that following a notifiable privacy breach, an organization must notify the NZ Privacy Commissioner as soon as practically possible (Parliamentary Counsel Office, n.d.-a). Note

that the act defines a “notifiable privacy breach” as one that is likely to cause “serious harm” (Parliamentary Counsel Office, n.d.-b).

NZ Privacy Act 2020 Data Breach Fines: If an organisation fails to notify the NZ Privacy Commissioner of a notifiable breach, then under Section 118, the organisation is subject to a fine which we outline in the next question of this section where we discuss the penalties of non-disclosure.

Ethical Considerations

As has been outlined from an analysis of national and international law, data breaches have the potential to cost the organization under consideration, Google, significant monetary loss. Not only this, but reputational damage is another deterrent for a business when considering disclosing a breach event (Putt, 2020, "NZ law is a lighter touch than other jurisdictions" section). This is supported by a survey showing almost 87% of those who had doubts about how responsible an organisation was around securing their data would look to other businesses (PwC, 2017, p. 2).

However, consideration of the effects on the lives of those who’ve had their personal data exposed offer another perspective in examining loss. As outlined in Recital 85 of the GDPR, victims of a personal data breach can suffer from anything from identity theft and fraud to substantial social disadvantage (*Recital 85 - Notification Obligation of Breaches to the Supervisory Authority*, 2019). Take the case of Claude Beland, former president of Desjardins Group. Scammers were able to use personal breached data to steal money from three separate companies using his social insurance number (Harris, 2019). Identity theft events happened to 5.66% of data breach victims in 2017 (Hays, 2020, "What is identity theft?" section). Let us speculate that a comparable percentage of the 1.5 billion users will be victims of identity theft. It follows that the lives of approximately 85 million would be at risk under this scenario. Given the context of unprecedented worldwide challenges faced by many

today, reputational and monetary loss to a business should be considered hand in hand with the loss that has been shown to be seen by the many who have their personal data revealed to scammers.

Question 2

As was mentioned in the previous question, the penalties for failing to disclose notifiable data breaches is the issuing of fines by a relevant authority. We now outline these fines below.

GDPR Penalties

The fines fall under a two-tiered system (*GDPR – Official Legal Text*, 2019, Chapter 8, Art. 83(4-5)):

1. ***Tier 1***: fines of up to 10 million EUR or 2% of the global annual turnover, whichever is higher
2. ***Tier 2***: fines of up to 20 million EUR or 4% of the global annual turnover, whichever is higher

The allocation of the fine amount is left at the discretion of corrective authorities, with more severe violations receiving the second tiered fine (*GDPR – Official Legal Text*, 2019, Chapter 6, Art. 58(2i)).

CCPA Penalties

Similar to the GDPR, we see a two-tiered fine system:

1. ***Tier 1:*** Up to $2,500 for each unintended violation
2. ***Tier 2***: Up to $7,500 for each intentional violation

These fines exclude those which come by way of consumers suing for between $100and $750 per violation (*Bill Text - SB-1121 California Consumer Privacy Act of 2018.*, 2018, Chapter 735, Section 1798.150(A))

NZ Privacy Act 2020 Penalties

The NZ Privacy Act 2020 states that the penalty for failing to notify the NZ Privacy Commissioner of a notifiable data breach is up to $10,000 (Parliamentary Counsel Office, n.d.-c).

Marriott International Data Breach

In a statement issued by the Information Commissioner's Office (ICO), it was revealed that Marriott International had been issued a 99 million EUR fine for breaching the GDPR (Information Commissioner's Office, 2019). The statement outlines that the core of the violation was a failure of proper due diligence, as Marriott had acquired the already compromised systems of Starwood hotels group in 2016, yet only became aware of the breached data they subsequently owned in 2018 (Information Commissioner's Office, 2019, para. 4).

Question 3

Recall the assignment case study describes how it was a Google employee who fell victim to a phishing attack after clicking on some malware that ultimately caused the data breach. An event such as this is sure to cause significant stress to this employee, as others have lost jobs as a result (INKY, n.d., para 1) and have had to pay legal fees to prove their innocence (INKY, n.d., para. 8). This was the unfortunate case of Patricia Reiley of Peebles Media Group, who was both fired, and sued for $138,000 for falling for a spear phishing campaign involving wiring money to scammers. However, the fine against Patricia was never

realised as the judge accounted for the fact that she had no cybersecurity training and the complexity of the adversary's methods (INKY, n.d., para. 5).

To come back to the Google case in question, any work-related impacts as a result of falling victim to phishing should be outlined in the company's Human Resources (HR) policies. If a policy states that their employment be terminated in an event such as the one described, the victim must oblige to the ending of their employment with Google. However, as was seen in the case of Reiley, the victim must also be prepared in the event that Google chooses further legal action. Reiley avoided fines due to her lack of training, however if the victim in question was given training aiming to prepare them for exactly the type of phishing scam they fell for, this could be argued as negligence on the victims part which could lead to similar legal action seen in the Reiley case.

Section 2

Question 1

It has been said by various security researchers that the line between a penetration tester and an adversarial hacker is permission (Kassner, 2015, para. 2). Considering this, any penetration test requested by the CISO of Google should be outlined in a legally binding document to protect both the penetration tester, and the business requesting the penetration test (pentest), as suggested by Kassner (2015, "Treat the audit agreement as a professional services engagement" section). Kassner also suggests two critical points:

1. Do not perform any tests which have not been agreed upon in the pentest document (Kassner, 2015, para. 8). In other words, do not move out of scope of what has been defined by both the CISO and the penetration tester
2. As a penetration tester, seek to resolve vulnerabilities rather than create more (Kassner, 2015, para. 9). A high level of responsibility should be assumed by the tester, and their actions should reflect an obligation to ensure no added risk results from their tests.

Kassner goes on to surface computer crime laws which could apply to any occurance where an “attempt to access a computer or computer network without authorization or in excess of authorization” is a crime under 18 USC 1030 (Kassner, 2015, "Considerations for security auditors" section). This further illustrates the importance of having the aforementioned legal document outlining that 1) the penetration test requested is authorized, and 2) the penetration tester that will perform the test is authorized to do so.

Question 2A

Hackers can be classified into three main categories, commonly known as White Hats, Grey Hats, and Black Hats.

White Hats

White Hat Hackers are also known by the term, “ethical hackers” (Norton, 2017, "White Hat Hackers" section), and in that term reveals the inclination of this type of hacker. As stated previously, these security researchers are commonly found in penetration testing roles, as they operate on the critical requirement of businesses - permission. Their work often leads to the hardening of business systems which ultimately help keep adversarial actors out (Matia, 2021, "White Hat Hackers" section), commonly known as Black Hats.

Black Hats

Black Hat Hackers do not wait for the permission of those who own the systems they break into, and often their motivations range from financial extortion to looking for a surge of adrenaline (Norton, 2017, "Black Hat Hackers" section). The term ‘malware’ is often associated with Black hats who leverage them to illegally obtain the personal information of unsuspecting victims (Matia, 2021, "Black Hat Hackers" section).

Grey Hats

This breed of hacker consists of elements from both the White hat and Black hat (Norton, 2017, "Grey Hat Hackers" section), where they may not necessarily have the permission to investigate a system, however upon finding a vulnerability, will alert the system owners. Where they begin to move more towards the ethos of Black hats is the situation where, in their dissatisfaction with the response from disclosing their findings, they

themselves capitalise on the found vulnerability, or sell it to the Black hat community (Matia, 2021, "Grey Hat Hackers" section).

Question 2B

The recommendation to the CISO regarding payment of the requested ransom in order to obtain the lost data is not to pay the hackers. This is based upon the fact that previously seen extortions which used a data breach as GDPR violation blackmail saw attackers either request more money after a payment, or no delivery of data whether the ransom is paid or not (Abrams, 2020, "Uses GDPR violations as extortion strategy" section). Kaspersky (2020, “Looking Ahead” section) also recommended that organizations remember the criminal nature of ransomware, refuse to pay the ransom, and instead alert the authorities to provide guidance on next steps.

Conclusion

This report investigated the legal and ethical factors surrounding the case study of a data breach of Google customers caused by malware via a phishing attack. As the reach of Google is global, both national and international laws had to be considered, as data protection laws have been developed in the modern world to help keep its citizens safe in the ever-changing landscape of the Internet. An analysis into work-related and legal implications for the victim of the phishing attack was conducted, where HR policies were found to be a critical document to guide the course of said victim. We also explored resulting legal ramifications of failing to protect citizens as a result of a data breach, as well as potential ramifications for conducting further investigations by way of penetration testing. Finally, the ethics of the three main categories of hackers was discussed, and a recommendation of no payment to the attackers responsible for the phishing attack on Google was provided to the CISO based on evidence from previous extortion cases, as well as a survey from a notable cybersecurity vendor.

References

Abrams, L. (2020a, July 2). *Surge of MongoDB ransom attacks use GDPR as extortion leverage*. BleepingComputer. https://www.bleepingcomputer.com/news/security/surge-of-mongodb-ransom-attacks-use-gdpr-as-extortion-leverage/

Abrams, L. (2020b, July 2). *Surge of MongoDB ransom attacks use GDPR as extortion leverage*. BleepingComputer. https://www.bleepingcomputer.com/news/security/surge-of-mongodb-ransom-attacks-use-gdpr-as-extortion-leverage/

Bill Text - SB-1121 California Consumer Privacy Act of 2018. (2018, September 24). California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

EDPB. (2020, March 11). *The Swedish Data Protection Authority imposes administrative fine on Google | European Data Protection Board*. https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en

GDPR – Official Legal Text. (2019, September 2). GDPR. https://gdpr-info.eu/

Google. (n.d.). *From the garage to the Googleplex*. about.google. Retrieved May 2, 2021, from https://about.google/our-story/

Harris, C. (2019, July 13). *Former Desjardins president falls victim to identity theft after data breach*. CBC.

https://www.cbc.ca/news/canada/montreal/desjardins-former-president-identity-theft-data-breach-1.5210717

Hays, C. (2020, January 29). *The Ultimate Guide to Data Breaches and Identity Theft*. Bloom Blog. https://bloom.co/blog/ultimate-guide-to-data-breaches-and-identity-theft/#what-is-identity-theft

Information Commissioner's Office. (n.d.). *Personal data breaches*. ICO. Retrieved May 2, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Information Commissioner's Office. (2019, July 9). *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*. ICO. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

INKY. (n.d.). *Employees Falling for Phishing Scams: Who is at Fault?* Retrieved May 4, 2021, from https://www.inky.com/blog/employees-falling-for-phishing-scams-who-is-at-fault

Kaspersky. (2020). *Ransomware Revealed: Paying for the Protection of your Privacy*. https://media.kasperskydaily.com/wp-content/uploads/sites/85/2020/03/25170451/Final_Ransomware-Report.pdf

Kassner, M. (2015, October 29). *Don't let a penetration test land you in legal hot water*. TechRepublic.

https://www.techrepublic.com/article/dont-let-a-penetration-test-land-you-in-legal-hot-water/

Law section. (n.d.). California Legislative Information. Retrieved May 2, 2021, from https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.81.5

Matia, L. (2021, February 5). *White Hat, Black Hat, and Grey Hat Hackers: What Do They Do, and What Is the Difference Between Them?* The State of Security. https://www.tripwire.com/state-of-security/security-data-protection/white-hat-black-hat-and-grey-hat-hackers-difference/

Norton. (2017, July 24). *What is the Difference Between Black, White and Grey Hat Hackers?* https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Parliamentary Counsel Office. (n.d.-a). *Privacy Act 2020 No 31 (as at 01 April 2021), Public Act 112 Interpretation – New Zealand Legislation*. New Zealand Legislation. Retrieved May 3, 2021, from https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23502.html

Parliamentary Counsel Office. (n.d.-b). *Privacy Act 2020 No 31 (as at 01 April 2021), Public Act 114 Agency to notify Commissioner of notifiable privacy breach – New Zealand Legislation*. New Zealand Legislation. Retrieved May 2, 2021, from https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23503.html

Parliamentary Counsel Office. (n.d.-c). *Privacy Act 2020 No 31 (as at 01 April 2021), Public Act 118 Offence to fail to notify Commissioner – New Zealand Legislation*. New

Zealand Legislation. Retrieved May 3, 2021, from https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23508.html

Putt, S. (2020, July 5). *What CIOs need to know about NZ's 2020 Privacy Act reforms*. CIO NZ. https://www.cio.com/article/3565173/what-cios-need-to-know-about-nz-s-2020-privacy-act-reforms.html

PwC. (2017). *Consumer Intelligence Series: Protect.me*. https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

Recital 85 - Notification Obligation of Breaches to the Supervisory Authority. (2019, September 3). General Data Protection Regulation (GDPR). https://gdpr-info.eu/recitals/no-85/

Vanderbilt University, & Schmidt, D. C. (2018, August). *Google Data Collection*. Digital Content Next. https://static.poder360.com.br/2018/08/DCN-Google-Data-Collection-Paper.pdf