LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS5052NI Professional Issues Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2021-22 Spring / 2021-22 Summer

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: May 12, 2022

Assignment Submission Date: May 12, 2022

Word Count: 3008

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Abstract

Data breaches occur because of various reasons. The most common reasons for a data breach is usually lack of implementation of proper preventive measures, handling the system improperly, using outdated technology and softwares and so on. This report aims to provide a case study of the data breach where an online casino group leaked information which included various sensitive information about the customers. This breach is significant because the Elasticsearch database which was leaked contained information of more than 5 billion records. This report elaborates about the various legal, social, ethical, and professional issues which arose due to this event. It also suggests ways in which the effects of such a disaster can be minimized so that such incidents do not manifest again in the future.

Table of Contents

Abstract i

Table of Contents ii

Table of Figures iv

1. Introduction 1

    1.1 Background of the leak 2

    1.2 Timeline of the data breach 3

2. Legal Issues 4

    2.1 General Data Protection Regulation (GDPR) 4

    2.2 Data Breach Notification Act 4

    2.3 Electronic Communications Privacy Act (ECPA) 4

    2.4 Computer Fraud and Abuse Act (CFAA) 5

    2.5 Computer Misuse Act (CMA) 5

3. Social Issues 6

    3.1 Economic Loss 6

    3.2 Reputational Damage 6

    3.3 Psychological issues 6

    3.4 Decline in trust towards companies 7

    3.5 Identity Theft 7

4. Ethical Issues 8

    4.1 Gambling 8

    4.2 No reimbursement for the clients 8

    4.3 Lack of proper security measures 8

    4.4 Unfair loss for the clients 9

    4.5 Lack of probity of the organization 9

5. Professional Issues 10
5.1 Unexpected Expenses 10
5.2 Poisoned search results of the corporate brand 10
5.3 ACM code of ethics and professional practice 10
5.4 Operational Downtime 11
5.5 Legal repercussions 11
6. Conclusion 12
7. References 13

Table of Figures

Figure 1: 108 million bets at various online casinos leaked 1
Figure 2: More than 5 billion records exposed through Elasticsearch server 2
Figure 3: A small portion of the redacted user data leaked by Elasticsearch server 3

1. Introduction

In January 2019, more than 108 million wagers were leaked by an online casino community, including personal information and transactions which was published by ZDnet. The information was obtained from an ElasticSearch server that had been left open without a password. ElasticSearch is a search engine which is portable and has high-performance. With the help of this tool, the search capabilities and data indexing of online applications can be enhanced by the companies. The user data included sensitive information such as real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP addresses, browser and OS details, last login information, and a list of played games, according to Justin Paine, the security researcher who discovered the server (Cimpanu, 2019).

Figure 1: 108 million bets at various online casinos leaked

(Abrams, 2019)

Elasticsearch servers have continued to leak millions of people's and organization’s protected personal data. Bithouse, the app developer for Peekaboo, left the Elasticsearch database open, revealing over 70 million log files holding almost 100 GB of data going back at least to March 2019. The data included detailed hardware data, URLs to images and videos, and almost 800,000 e-mail addresses. Elasticsearch servers have long been a security concern. When there are no passwords or firewalls, security experts say, a breach happens due to a lack of built-in protective measures. Secure authenticated sign-in, strong encryption, multilayered safeguards, and logs of audit are among ElasticSearch's security recommendations. (Cisomag, 2021).

1.1 Background of the leak

Following the accidental leak of a U.K.-based security firm's "Data Breach Database," which held vast volumes of data tied to security incidents from 2012 to 2019. A total of 5,088,635,374 records (more than five billion) were exposed. Bob Diachenko, a security researcher, found the hacked database. Diachenko reported that the leaked database contained a large amount of previously known and unreported security event details, including Hashtype (the method a password was presented: MD5/hash/plaintext, etc.) and Leak date (year), Password (hash, encrypted, or plaintext depending on the breach), Email, Email domain, and Leak Source. Diachenko asserted that he was able to verify some of the well-known security breaches on LinkedIn, Adobe, Twitter, Last.fm, VK, Tumblr, and other platforms. After Diachenko quickly submitted a security notice, the database was taken offline within an hour (Cisomag, 2021).

Figure 2: More than 5 billion records exposed through Elasticsearch server

(Immanni, 2020)

The researcher found after a comprehensive examination that the unprotected engine was built by an aggregation online gambling firm that operates multiple casino and sports betting websites under its umbrella, including viproomcasino.net, kahunacasino.com, easybet.com, and other brands. Mountberg Limited, situated in Limassol Avenue, Nicosia, Cyprus, owns and operates the bulk of the above-mentioned websites, which operate under a Curacao eGaming license and are

regulated by the Caribbean island's government. The remainder of the brands, on the other hand, are owned by a completely other company, such as TGI Entertainment NV, which is also based in Cyprus (Abrams, 2019).

```
      },
      "method": "creditcard",
      "forgotten": false,
      "id": "40eecc3d-785d-4fe5-8793-a778ff43e523",
      "maskedAccount": "XXXXXX******XXXXX",
      "processor": "paymentiq",
      "favorite": false
    }
  ],
  "metadata":
  "{\"fname\":\"XXXXXXXX\",\"lname\":\"XXXXXXXX\",\"birthdate\":\"1980-XX-XXT00:00:00.000Z\",\"addres
  s\":\"12 XXXXXXX
  Avenue\",\"zip\":\"2XXX\",\"city\":\"MiddleXXXXXX\",\"countrycode\":\"au\",\"username\":\"XXXXXXX8080\
  ",\"email\":\"XXXXXXXXX@gmx.com\",\"password\":\"********\",\"password_confirm\":\"********\",\"cur
  rencycode\":\"AUD\",\"phone\":\"+610XXXXXXXXX\",\"countries_prefix\":\"+61\",\"language\":\"en\",\"id\"
  :\"4505221\",\"portalId\":\"39\"}",
  "lastActive": "2019-01-19T04:59:14.227895",
  "portalId": "5a5c578b90330398a6d245cc",
  "fingerprint": "f1721a2fbd982849b2ec8ceeXXXXXXXXXX",
  "isOnline": true,
  "id": "5c41552471a11e001a7b1995"
},
"affiliate": {
  "system": "gofiliate",
  "portalId": "39",
  "id": "gofiliate_39_28",
  "affiliateId": "28",
  "affiliateToken": "goa_b99f66d5-f87b-4ce4-a495-21db58c81fa6",
  "email": "XXXXXXXX@XXXXXXXXXX.com",
  "username": "XXXXXXXX_18"
},
"depositAmount": 1250.0,
"depositAmountEUR": 788.9411890744582,
```


Figure 3: A small portion of the redacted user data leaked by Elasticsearch server

(Abrams, 2019)

1.2 Timeline of the data breach

While it is uncertain whether the disclosed data was used by any intruders, the researchers claim that the database was open for a minimum of 4 days. The order of incidents is:

- **May 28, 2021**: Search engines indexed the database.
- **May 29, 2021**: Diachenko found the breached database and informed Cognyte..
- **June 2, 2021**: The database was secured by Cognyte.

(Cisomag, 2021)

2. Legal Issues

2.1 General Data Protection Regulation (GDPR)

Article 57 of the GDPR and Section 115(2)(a) of the DPA 2018 impose a wide variety of legislative tasks on the Commissioner, including monitoring and enforcing the GDPR, promoting good practice, and ensuring that those who process personal data comply with data protection requirements. These responsibilities are in addition to those imposed by the various enforcement regimes. This requirement could not be met by the online casino companies which violated the law as they could not protect the personal information of their clients (Information Commissioner's Office, 2019).

2.2 Data Breach Notification Act

The Data Breach Notification Act of 2010 is a legislation that requires persons or companies impacted by a data breach, such as illegal access to data, to inform their clients and stakeholders about the breach, as well as take particular actions to fix the problem depending on state law. There are two basic aims to data breach notification legislation. The primary purpose is to provide people the opportunity to reduce their risk of data breaches. The second objective is to encourage companies to improve data security. These objectives work together to reduce the impact of data breaches on consumers, such as impersonation, fraud, and identity theft (Senate Judiciary Committee, 2022).

2.3 Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) of 1986 forbids interception of email and viewing of stored email without a court warrant. However, there is an exemption for business systems, which states, employers are not prohibited from viewing employee correspondence stored on business networks. Since the database was exposed online the stored information about clients email and various other relevant information was left visible on the internet. Thus, the this data breach violates the ECPA (Baase & Henry, 2018).

2.4 Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) of 1980 is a federal law that covers areas where the federal government has authority, such as government computers, financial systems, and computers used in interstate or international commerce or communication—the latter category, of course, includes computers connected to the Internet, mobile phones, and other similar devices. It is prohibited under the CFAA to read or copy information from such a device without authorisation, or to exceed one's authorization. Altering, corrupting, or deleting information, as well as interfering with permitted computer usage, are all covered under the law. The CFAA is the primary anti-hacking law, although prosecutors can also utilize other federal statutes to punish anyone for offenses involving computers and telecommunications systems. Access to conduct fraud; revealing passwords or other access codes to unauthorized persons; and stopping or hindering government operations, public communication, transit, or other public services are all examples of illegal activities. Anti-hacking legislation on both the state and federal levels impose harsh penalties, including prison terms and fines (Baase & Henry, 2018).

2.5 Computer Misuse Act (CMA)

The Computer Misuse Act of 1990 establishes three different crimes: Unauthorized computer access, including the illegal copying of software stored on any computer. A magistrate will hear the case, which carries a penalty of up to six months in jail or a £5000 fine. Unauthorized access with the aim to conduct or enable the commission of further offenses (such as fraud or theft), which includes more serious examples of criminal hacking. This carries a maximum punishment of five years in jail and an infinite fine. It will be a jury trial because it is a severe felony (12 jolly good people). The purposeful and unlawful destruction of software or data; the online distribution of "infected" items ("viruses"); and the unauthorized insertion of a password to a data file ("crypto viruses"). This crime carries a maximum sentence of five years in jail and a fine of unspecified amount. Because it is a severe crime, a jury trial will be held (Osborne, 2006).

3. Social Issues

3.1 Economic Loss

A data breach's financial impact is certainly one of the most immediate and serious consequences that firms will face. Compensation for impacted consumers, incident response activities, investigation of the breach, investment in new security measures, legal expenses, and regulatory fines for non-compliance with the GDPR (General Data Protection Regulation) are just some of the costs that might be incurred. Such a huge loss for big companies could mean that many of the people could lose their jobs creating unemployment in the society and a poor financial situation.

3.2 Reputational Damage

Consumers understand the importance of their personal information, and if companies do not show that they have initiated the necessary efforts to protect it, the customers will turn towards their competitors who are more concerned and have taken measures to safeguard their data. When a company's reputation is destroyed, it loses its ability to attract new customers, future investment, and new employees (Metacompliance, 2020).

3.3 Psychological issues

After witnessing a breach of such magnitude, people become concerned about their privacy. A data leak such as this could expose their personal information including their phone numbers, addresses, etc. which could be a safety concern for most people. If such information gets published on the internet, then people have to live worrying that someone might cause severe damage to them. If people become paranoid and hesitate to use technology, then the rate of advancement could be slowed down.

3.4 Decline in trust towards companies

Employee turnover will occur as a result of a data breach, particularly at the executive level. Because of the consequences of the breach, some people will be dismissed. Others will quit due to the stress that comes with dealing with the incident. Blame and conflict are often passed down the ranks, resulting in turnover of employees. The corporation will have to replace those personnel, which could be difficult. Anyone who joins the firm as an executive must begin with the clean-up after an incident. IT and security professionals can afford to decline a job offer from a firm with improper security. This complicates the task of the human resources department and prolong the mitigating period.

3.5 Identity Theft

The implications of a data breach that results in the loss of sensitive personal data can be disastrous. Any information that may be used to identify an individual directly or indirectly is considered personal data. Everything from a name to an email address, IP address, and photographs are included. It also includes sensitive personal data like biometric or genetic information that might be used to identify a person. When the information of someone is used by another person, the identity of that individual gets stolen and can be used to commit notorious and wrongful acts. This puts the name of the victim in bad standing in the society.

4. Ethical Issues

4.1 Gambling

The acts of placing bets and gambling can be quite lucrative for the players who win the prize. But for the people who lose, they go in loss. The nature of gambling is such that, the players who lose, think that they will get lucky in the next game and place the bets, causing them to lose even more money. There are hundreds and thousands of people who gamble, the possibility of each individual making a profit out of it is non-existent. In such scenarios, there are more losers than winners which goes against the ethical theory of utilitarianism.

4.2 No reimbursement for the clients

After the data got breached, various sensitive information of the people connected with the company was left open on the internet. The clients who had their data stolen and misused, were not compensated in any way. According to the ethical principle of beneficence, the company should have taken action in a way which would benefit the majority. But they could not repay the clients for their loss. Thus, their actions contradict the ethical principle of beneficence.

4.3 Lack of proper security measures

The lack of adequate awareness for security of the server by employees caused the server to be hacked, which resulted in the data breach of over 5 billion records. Since the company had collected sensitive information from millions of people, they should have been more responsible and highly careful with how they handled the data, where it is stored and how it should be secured. The ignorance for the proper security of the data of its customers violated the ethical theory of deontology as the company could not provide safety for the customers' data. The company is obliged to provide security for their clients' information, and it is the duty of the employees to fulfil them which they could not maintain. Thus, the company went against the deontological theory.

4.4 Unfair loss for the clients

The carelessness of the company impacted the data of 5 billion records. Because of this, the data of the people got stolen and misused. The company could not provide justice for these people who got robbed of their identity and personal information. Justice is one of the most important aspects for maintaining equanimity in a society. If the people have to go through unjust situations there can be no morality. Thus, this defies one of the most fundamental ethical principles of justice.

4.5 Lack of probity of the organization

The lack of integrity which the organization displayed by allowing the confidentiality, integrity and availability of its data to be compromised not due to their incompetence but due to their ignorance. This irresponsible and inconsiderate behaviour exhibited by the organization goes against the ethical theory of virtue. The organization proved themselves not trustworthy and respectable which contradicts the virtue theory.

5. Professional Issues

5.1 Unexpected Expenses

The Chief Financial Officer (CFO) is in charge of keeping the organization on track financially. A data leak puts the budget into disarray. If the firm has cybersecurity insurance, it may be able to cover some of the unforeseen expenditures, but the Harvard Business Review warns that many businesses are either underinsuring or not insuring at all. Even if insurance is in place, cyber event claims are difficult to file and may not cover the expenses. There is also the issue of lost revenue during downtime (Poermba, 2021).

5.2 Poisoned search results of the corporate brand

After a cybersecurity event, the chief marketing officer (CMO) will realize that nothing actually vanishes on the internet. Some businesses' reputations will be tarnished permanently as a result of a data leak. That remains true regardless of how long ago it occurred. After an event, the damage will take months, if not years, for CMOs and marketing departments to restore. They will have to fight every Google search that contains the firm name and the phrase "data breach".

5.3 ACM code of ethics and professional practice

As an ACM member the employees take an oath to contribute to society and human well-being, avoid harm to others, be honest and trustworthy, be fair and take actions not to discriminate, honour proprietary rights including copyrights and patent, give proper credit for intellectual property, respect the privacy of others, honour confidentiality and many other such promises to work honestly and provide for the community. However, in due course of the breach several of these values were violated when the breach occurred, and the client’s information was compromised.

5.4 Operational Downtime

Network outages cost an average of $5,600 every minute. Every hour, this amounts to about $300,000. This will vary depending on the size of the firm and the type of business, but it will almost certainly have a negative influence on the efficiency of the company. During this time, the company could not provide services to its clients who were a part of the company and used their services on a daily basis. This hampered the customers' experience with the organization.

5.5 Legal repercussions

In the aftermath of the breach, the legal team also has to deal with the necessary repercussions. They must guarantee that state and federal consumer notification rules are followed. Organizations that interact with a worldwide consumer base must likewise deal with the consequences of global data privacy infringements. If the breach results in litigation, the legal team have to devote weeks or even months to crafting statements and reviewing production data and forensic investigations in order to find anything that can help the business defend itself. A data breach is more than a single instance of sensitive data being compromised. More than the IT and security teams are responsible for its mitigation. The consequences affect everyone in the firm, starting with the CEO.

6. Conclusion

As businesses migrate to cloud providers to store their databases, data breaches are becoming more common. The databases may contain not just private information about the businesses, but also personally identifiable information about their customers. Because information is more easily available to be exposed, data breaches are on the rise. An attacker can remotely disclose vulnerabilities to a cloud platform instead of being in a local data center. As a result, millions of individuals linked with the targeted organization suffer. This report provides an overview of what a data breach is and how it might affect any company. Even the major corporations, which are relied on by billions of people are very much susceptible to such incidents.

Even though it is clear that human error is at the root of major problems, prominent corporations continue to make the same mistakes that affect billions of individuals who use their services. This report demonstrates that data breaches are not limited to small businesses. In fact, they may also occur to organizations including well-known banks and larger companies. Billions of people will live a better life and not have to worry about sensitive data being abused if they are aware of the key problem with data breaches and are further educated on how to avoid being exploited.

The most typical sort of breach in Elasticsearch is when a cluster is left unprotected on the internet, allowing any individual to login without account details such as email id and passphrase to view the data. A company can set up security for their Elasticsearch cluster and avoid data breaches by doing so. The simplest way to ensure that others do not have access to an organization's Elasticsearch clusters is to enable authentication so that no one can access their Elasticsearch without first logging in. Also, to prevent eavesdropping on Elasticsearch data flowing via company's network, Transport Layer Security (TLS) should be enabled. And most importantly, the data should not be stored in plain text. Instead, it should be encrypted with a strong encryption algorithm so that anyone who comes across it cannot easily view its contents.

7. References

Abrams, L., 2019. *Online Casino Database Leaks Details of Over 100 Million Bets.* [Online] Available at: https://www.bleepingcomputer.com/news/security/online-casino-database-leaks-details-of-over-100-million-bets/
[Accessed 2 May 2022].

Baase, S. & Henry, T. M., 2018. *A gift of fire: social, legal, and ethical issues for computers and the internet.* 5th ed. New York: Pearson.

Cimpanu, C., 2019. *Online casino group leaks information on 108 million bets, including user details.* [Online]
Available at: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/
[Accessed 26 April 2022].

Cisomag, 2021. *5 Bn Records from Previous Data Breaches Leaked.* [Online] Available at: https://cisomag.eccouncil.org/another-case-of-unprotected-database-5-bn-records-from-previous-data-breaches-leaked/
[Accessed 1 May 2022].

Immanni, M., 2020. *15,000 Elasticsearch Servers Are Attacked and Wiped By Unknown Hacker.* [Online]
Available at: https://techdator.net/15000-elasticsearch-servers-are-attacked-and-wiped-by-unknown-hacker/
[Accessed 24 April 2022].

Information Commissioner's Office, 2019. *Memorandum of Understanding between the Information Commissioner and the Gambling Commission.* [Online]
Available at: https://ico.org.uk/media/about-the-ico/documents/1560121/mou-gambling-commission.pdf
[Accessed 28 April 2022].

Metacompliance, 2020. *5 Damaging Consequences Of A Data Breach.* [Online] Available at: https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/
[Accessed 25 April 2022].

Osborne, M., 2006. *How to Cheat at Managing Information Security.* 1st ed. Waltham: Syngress.

Poermba, S., 2021. *6 Potential Long-Term Impacts of a Data Breach.* [Online] Available at: https://securityintelligence.com/articles/long-term-impacts-security-breach/ [Accessed 1 May 2022].

Senate Judiciary Committee, 2022. *DATA BREACH NOTIFICATION ACT,* Washington DC: Library of Congress.