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

2022-Spring

Student Name: Nabina Limbu

London Met ID: 20048926

College ID: NP01CP4S210314

Assignment Due Date: May 12 2022

Assignment Submission Date: May 12 2022

Title (Where Required):

Word Count (Where Required): 3740

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.

Table of Contents

Table of Figures

Introduction

ZDNet is a company-generating information site owned and operated by Red Ventures. The Emblem was founded on April 1, 1991, as a popular hobby generation site by Ziff Davis and evolved into a company IT-targeted online publication. ZDNet began as a subscription-primarily based virtual provider known as "ZiffNet" that delivered computing data to CompuServe customers. It had searchable archives, laptop enterprise forums, events, and features. ZiffNet was created with the intention of serving as a central repository for information from all Ziff-Davis print periodicals.

As a result, ZiffNet expanded into a sophisticated web provider known as PCMagNet for PC Magazine readers. PCMagNet, which launched in 1988, evolved from Ziff Davis' first digital publishing venture, a bulletin board, which debuted in 1985. Ziff-Davis announced the merging of their online record products under a single moniker, ZDNet, on June 20, 1995. The company had 275,000 subscribers across six platforms: CompuServe, Prodigy, AT & T Interchange, Microsoft Network, AppleLink, and eWorld.

Figure 1: ZDnet

ElasticSearch is a distributed, free, and open search and analytics engine that can handle textual, numerical, geographic, structured, and unstructured data. ElasticSearch is based on Apache Lucene and was initially published by ElasticSearch N.V. in 2010. (Now known as Elastic). Elasticsearch is the key component of the Elastic Stack, a collection of free and open tools for data intake, enrichment, storage, analysis, and visualization. It is known for its easy REST APIs, distributed nature, speed, and scalability. The Elastic Stack (after ElasticSearch, Logstash, and Kibana) now includes a comprehensive array of lightweight shipping agents known as Beats for transferring data to ElasticSearch (ElasticSearch, n.d.).

Since its launch in 2010, Elasticsearch has quickly become the most popular search engine, and it is frequently used for log analytics, full-text search, security intelligence, business analytics, and operational intelligence use cases. Elasticsearch receives raw data from a number of sources, including logs, system metrics, and web applications. Data ingestion is the process of parsing, normalizing, and enriching raw data before indexing it in Elasticsearch (ElasticSearch, n.d.). Once their data is indexed in Elasticsearch, users may perform complicated queries against it and utilize aggregations to generate elaborate summaries. Users may utilize Kibana to build powerful data visualizations, share dashboards, and manage the Elastic Stack.

Figure 2: Elastic Search

Background

There has been much debate regarding the internet and its privacy. Some argue that whatever you do on the internet today violates your privacy. They claim that the government is eroding citizens' privacy by monitoring everything that happens on the internet. When web users give out their personal information on the Internet, Internet privacy comes into the picture. On certain websites, which facilitate online shopping, users are made to input their credit card numbers. In the case of email sites, there is debate about whether third parties should be permitted to keep or access communications without informed consent. So, do you believe the information we provide to an online organization is safe? Do they consider our privacy?

In January 2019, ZDnet revealed that an online casino group leaked information on more than 108 million bets, including details about customers' personal information, deposits, and withdrawals. The information was leaked from an ElasticSearch server that had been left open to the public without a password. According to ZDNet, the data was exposed due to a misconfigured Elasticsearch database. Data from websites such as kahunacasino.com, azur-casino.com, easybet.com, and viproomcasino.net was accessed.

The companies were not identified, but a short web search reveals that one of the sites, Easybet, is owned by TGI Entertainment NV, a Curacao-based company. Another is owned by Mountberg Ltd., a Cyprus-based firm. Customers' credit card information, full names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, IP addresses, browser and OS details, last login information, and other information were exposed.

The breach, according to Mark Weiner, chief marketing officer of Balbix Inc., is just another example of a prevalent trend: a business leaving a server and vital information exposed with no password security. This is the source of numerous recent leaks, including the VOIPo and Oklahoma Securities Commission instances (Duncan, 2019). He believes the data might be utilized by malicious actors as part of a phishing scheme targeting people who have just won huge sums of money. The good news is that the leaked credit card data was partially redacted, which means that consumers' entire financial information was not revealed.

Legal Issues

Legal issues arise within the normative framework established and enforced by legal authorities and institutions. While regulations, directives, and rules address specific societal issues, fundamental rights and values guide their application at a higher level of abstraction. In this sense, the law may be viewed as an attempt to solve societal problems through the institutionalization of processes for developing, enforcing, and resolving norm conflicts. As a result, legal issues might arise when new situations, such as new technology, contradict old legal interpretations. This issue might be addressed at the level of legal doctrine and the application of standards in court cases or government legislation. It may also lead to the realization that the present legal structure no longer meets the aims it set out to achieve and, as a result, must be changed to meet new conditions (Schroeder, et al., 2009).

In 2019 ZDnet found that millions of personal information including name, phone no, Gmail, and even the website that is used to log in was left open without any password and when they report about data breaching Elasticsearch says they have always provided some recommendations on how to secure their servers, which include secure authenticated sign-in, proper encryption, layered security, and audit logging. Elasticsearch servers have continued to leak millions of people's and organizations' protected personal information. They have failed to protect their customer’s data by doing so they violated some of the acts and laws they are:

- General data protection regulation (GDPR)

  The General Data Protection Regulation (GDPR) is the world's toughest privacy and security regulation. Though it was designed and enacted by the European Union (EU), it imposes restrictions on organizations anywhere that target or collect data about EU citizens. On May 25, 2018, the regulation came into action (Wu, 2022). GDPR covers a wide range of "personal data," which includes information about an identified or identifiable natural person, such as names, health information, financial information, email addresses, and even IP addresses, phone numbers, and device identifiers. The GDPR also compels businesses to notify everyone who has been affected by a data breach within 72 hours of becoming aware of it.

Since elasticSearch has failed to protect the privacy of their customers by leaking their information they have violated the privacy and security standards of GDPR. The penalties for breaking the GDPR are severe. There are two levels of sanctions, with a maximum fine of €20 million or 4% of worldwide turnover (whichever is higher), plus parties involved have the right to seek compensation for damages.

- Gramm-Leach-Bliley Act

ElasticSearch violated the Gramm-Leach-Bliley Act by exposing personal information such as credit card information, full names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, and so on. The Gramm-Leach-Bliley Act (GLBA) simplifies key financial services sector rules. However, it imposes substantial privacy and security standards on financial organizations, as defined by the GLBA (Wu, 2022). The GLBA and its implementing legislation require financial institutions to protect their customers' privacy as well as the security and confidentiality of their customers' nonpublic personal information.

- Data breach notification law

ElasticSearch violated the law by failing to notify individuals about the exposure of their personal information on the internet. Regulations concerning how data breach notification laws should be applied, such as who the rules apply to and what constitutes a violation under these laws, are included. These regulations compel businesses that have been breached (and are covered by the Legislation) to notify the individuals whose data has been compromised, as well as other relevant parties, of the occurrence. Data breach notification laws also require companies that process data to implement data security measures and/or take efforts on the part of the affected firm to correct the problem and/or minimize the harm.

Social Issues

A social issue is any circumstance or behavior that has a negative impact on a significant number of people and is commonly recognized as a condition or behavior that needs to be addressed. If a social issue impacts a significant number of individuals in a public setting, it may be difficult to resolve. It might be a collection of prevalent problems in modern society that many people strive to solve. Social issues are the root of a competing evaluation based on what is morally acceptable or not in human life or social open action possibilities (R., 2011). Different societies have different conceptions of what "normal" behavior is, and what is "normal" behavior in one community may be a huge societal concern in another. Although social problems are distinct from monetary concerns, many issues (such as migration) have both social and financial elements. There are also options that do not fit within either category, such as fighting. In Rights of Man and Common Sense, Thomas Paine discusses man's obligation to "allow the same rights to others as we give ourselves." Failure to do so results in the development of a societal problem (Anon., 2020).

In this case of a data breach from an online organization, it impacts customers and businesses as well as our society, causing several unwanted troubles. Individuals who have had their information leaked may face difficulties such as frequent password changes, credit freezes, or identity monitoring, among other things. Identity theft poses a significant risk to data breach victims. Leaks of data may expose anything from social security numbers to financial details. Once a criminal obtains the information, they may commit any sort of fraud in your name. Identity theft may wreck your credit and get you in legal trouble, and it is tough to fight back. A person can lose their reputation, which took them years to build, due to personal information that is revealed because of data leakage. They may also face long-term debt as a result of online identity theft, which will result in a poor credit rating.

In today's hyper-connected society, information spreads instantaneously. Even those who have never heard of the business will almost definitely become aware of a breach within a few days. Because of the data breach, the company may suffer a number of consequences, some of which are as follows:

- **Financial Loss**

  There is no doubt that the financial impact of an infringement is one of the most immediate and harsh consequences organizations are to deal with. In the past five years, the cost of a breach of data has, according to a recent study by the Ponemon Institute, risen 12% to £3.2 million globally, by average. Costs may include compensating the customers affected, making incident reaction efforts, investigating the violation, investing in new safeguards, legal fees, and eye-watering regulatory sanctions that may be imposed for non-compliance with the GDPR (General Data Protection Regulation).

- **Reputational damage**

  The damage caused by a data breach can be devastating for a company. Research has demonstrated that up to one-third of retail, financial and health-related customers will stop working with violated organizations. Moreover, 85% tell other people what they are doing, and 33.5% take their anger to the welfare media. News travels rapidly and organizations can become a global news story within hours of a violation.

  The negative press and a loss of consumer confidence can cause the breached company irreparable damage. Consumers know all too much about the value of their data, and if organizations fail to show their efforts to protect these data, they will simply leave and go to a competitor who takes safety more seriously. The reputation damage is lasting and will also affect the ability of an organization to attract new customers, investment in the future, and new employees. Reputational damage also leads to customer loss and, as a result, a decrease in sales.

- **Operational Downtime**

  In the event of data breaches, business transactions are often seriously disrupted. Organizations will have to contain the breach and carry out a thorough study of how it happened and the systems they accessed. It may be necessary to shut operations down completely until researchers receive all the answers. Depending on the severity of the violation, this process may take days or even weeks. This can have a massive impact on revenue and a recovery capacity for an organization.

  The average network downtime cost, according to Gartner, is approximately $5,600 per minute. That is approximately 300,000 dollars an hour. This will of course be different depending on the size of the organization and the industry concerned, but it can clearly be detrimental and affect business productivity considerably.

- **Legal Action**

  Organizations are legally obliged to demonstrate, under data protection regulations that all necessary steps have been taken to protect personal data. When these data are jeopardized, whether or not it is intentional, people may seek compensation in law. In both the USA and UK, as victims seek monetary compensation on loss of their data, class action lawsuits have increased dramatically. More than 145 million people worldwide have been affected by the 2017 data breach of Equifax, which has paid over $700 million in compensation to the US customers affected. The violation affected an estimated 15 million UK customers who are now seeking compensation for their separate lawsuits in the High Court.

Ethical Issues

Ethical issues emerge when a specific choice, circumstance, or behavior contradicts the ethical standards of the general public. Both individuals and organizations may become caught in these disputes since any of their efforts may be directed at the problem from an ethical stance. These conflicts can be legally hazardous since some of the possibilities for settling the issue may fall under specific legislation. Despite the fact that the matter is unlikely to have arisen legally, it may provoke a negative reaction from untouchables. Ethical problems are difficult to address since no guidelines or points of reference have been established. As a result, many businesses have ethical standards that are researched and endorsed by significant individuals in order to create a framework for businesses and individuals to make acceptable choices whenever they face one of these issues.

Our ethics dictate that we must follow our morals and not destroy the property of others, and this online organization is not doing so; they are harming people's sensitive information on the internet, which anybody may access. According to John Stuart Mill's Utilitarianism theory, a person should act in order to provide benefits to most people or maximize happiness or pleasure while minimizing unhappiness or suffering. According to this argument, it is immoral to make many people unhappy, and elasticSearch is doing the same by leaking the personal details of its customers on the internet. The problem with ethical issues such as whether or not capital punishment should be permitted or the morality of euthanasia is that there is no universally accepted resolution. These ethical dilemmas are extensively discussed since the solution frequently boils down to personal preference or philosophy. Ethics can provide more than one response, and that response is not always universally accurate.

Also according to Immanuel Kant's theory of deontology, "human beings should be treated with dignity and respect since they have rights." Deontology say that every promise should be kept and everyone’s privacy should be protected. ElasticSearch failed to keep their customers' promises of keeping their information safe and protecting their privacy. Customers' privacy is no longer secure because their data is freely accessible on the internet.

In my personal opinion, it is not ethical and does not come to our morality. According to Aristotle's virtue theory, once you can picture what a good person is like, you should behave in every situation as you would expect such a person to behave. The term "virtue" is not just a technical term, but it is also rarely used in daily speech. Virtues are good personality attributes such as honesty and charity. In this scenario, the organization is not being honest with their users by not informing them that their data is freely available on the internet and that anyone can find out about them in a matter of seconds and use their information for harmful activities such as identity theft or fraud, reputational damage, or causing the reversal of pseudonymisation and loss of personal data confidentiality.

Professional Issues

Professional issues arise when issues associated with the law of polished methodological ability appear, which frequently occurs when the tacit rules of an expert advancement association are broken. One of the expert concerns is data insurance; court data is exceptionally fundamental and should be accessible to individuals from the associations' courts. Encroachment of data security may be a huge problem since vital court information might be leaked and utilized for other illicit reasons. Without agreement, delegates should be barred from sharing AU statistics and information with the public. The association would provide or consent to provide adequate collaboration to the support customer (F., 2005).

Professionalism in one's conduct, demeanor, and attitude in a work or business environment is required in every field. A person does not have to work in a certain field to demonstrate significant qualities and characteristics of a professional. Professionalism leads to workplace success, a favorable professional reputation, and a high degree of work ethic and excellence. Professional issues may arise if the organization violates a set of accepted standards, jeopardizes data security or a pair of critical information capabilities, or issues a misleading notification. Among the sensitive information released from the ElasticSearch server were real names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, IP addresses, browser and OS characteristics, last login information, and a record of played games.

According to the IEEE computer society, a company's code of conduct should emphasize public safety, health, and welfare, aim for ethical design and sustainable development techniques, protect the privacy of others, and swiftly disclose concerns that may threaten the public or the environment. ElasticSearch violated this code of conduct because it was unable to prioritize public safety and preserve its customers' privacy due to data leakage.

The company should be honest and trustworthy to its consumers, however elasticSearch was unable to do so because they failed to notify their customers about the data leakage. A professional must prevent any kind of harm, which includes any negative repercussions, especially when such consequences are severe and unfair. Customers are being harmed as a result of the disclosure of personal information due to elasticSearch. Unjustifiable bodily or mental harm, unjustified destruction or exposure of information, and unjustified damage to property, reputation, or the environment are all examples of harm.

Conclusion

This report is about the elasticSearch scandal that was revealed by ZDnet in January 2019. As a result, customers and the company faced legal, social, ethical, and professional issues. This is not the first time elasticSearch's data has been compromised. During 2020 alone, Avon's cosmetics giant had 19 million records accessible on an Elasticsearch database. Another incorrectly set bucket containing Family Tree Maker, an online genealogy service, resulted in the exposure of approx. 25GB of sensitive data. More than five billion records were then exposed after another Elasticsearch database was left vulnerable. Surprisingly, it contains a massive database of previously hacked user data from 2012 to 2019. A security researcher even calculated how long it would take hackers to find, attack, and exploit an unsecured Elasticsearch server that had been intentionally left online – eight hours.

The cloud is now viewed as a unique technology that must be utilized as a result of digital transformation. While cloud technologies have many advantages, irresponsible usage has serious implications. Failure to comprehend or refuse to recognize the security implications of this technology can have disastrous consequences for a company. As a result, it's necessary to acknowledge that, in the case of Elasticsearch, simply because a product is free and incredibly scalable doesn't mean you can disregard basic security recommendations and configurations. Furthermore, because data is often viewed as the new gold coinage, there has never been a greater need to monetise up-to-date data. The data of a server can be leaked in a variety of ways, including a password being stolen, hackers entering systems, or even an insider breaching from within the protected environment itself. The most prevalent is when a database is left online with no protection (even without a password), allowing anybody to view the contents. Cloud security is a joint duty of the company's security team and the cloud service provider; nonetheless, the business must undertake the necessary due diligence to setup and protect every area of the system appropriately in order to reduce any possible threats.

To successfully avoid Elasticsearch (or similar) data breaches, a different approach to data security is necessary, one that permits data to be a) safeguarded wherever it may reside, and b) managed on their behalf by whomever may be handling it. This is why a data-centric security paradigm is more appropriate, as it allows a company to safeguard data and utilize it for analytics and data sharing on cloud-based resources while it is secured.

One approach is to use standard encryption-based security. However, encryption solutions come with sometimes-complicated administrative overhead to handle keys. Furthermore, many encryption techniques are easily cracked. Tokenization, on the other hand, is a data-centric security solution that substitutes harmless representational tokens for sensitive information. This implies that even if the data slips into the wrong hands, the tokens have no apparent significance. Sensitive information stays secure, preventing threat actors from profiting from the breach and data theft.

GDPR and the current wave of data privacy and security regulations have raised customer awareness of what is expected when they provide sensitive information to service providers, making data protection more crucial than ever. If tokenization techniques had been used to mask the information in many of these Elasticsearch server leaks, criminal threat actors would have been unable to decipher the data—the information would not have been compromised, and the organization at fault would have been compliant and avoided liability-based repercussions.

This is a lesson for all the data business: if anybody believes their data is secure while "hidden in plain sight" on a "anonymous" cloud resource, the recent incidents with Elasticsearch and other cloud service providers should serve as a wake-up call to act now.

Bibliography

Anon., 2020. *Definitions.net.* [Online] Available at: https://www.definitions.net/definition/social+issues. [Accessed 8 May 2022].

Duncan, R., 2019. *SiliconAngle.* [Online] Available at: https://siliconangle.com/2019/01/21/108m-online-casino-customer-records-exposed-latest-case-misconfigured-database/ [Accessed 9 May 2022].

ElasticSearch, n.d. *ElasticSearch.* [Online] Available at: https://www.elastic.co/what-is/elasticsearch [Accessed 9 May 2022].

F., B., 2005. *Professional Issues in Information Technology.* , Stanford Street: British Catalauging in Publication.

R., S., 2011. *Media, crime, and criminal justice: Images, realities, and policies,* s.l.: Wadsworth Publishing Group.

Schroeder, R., Meyer, E. T. & Ziewitz, M., 2009. *Social, Ethical and legal issues in presence research and applications,* s.l.: s.n.

Wu, S., 2022. *Silicon Valley Law.* [Online] Available at: https://www.svlg.com/data-security-breaches-a-legal-guide-to-prevention-and-incident.html [Accessed 7 May 2022].