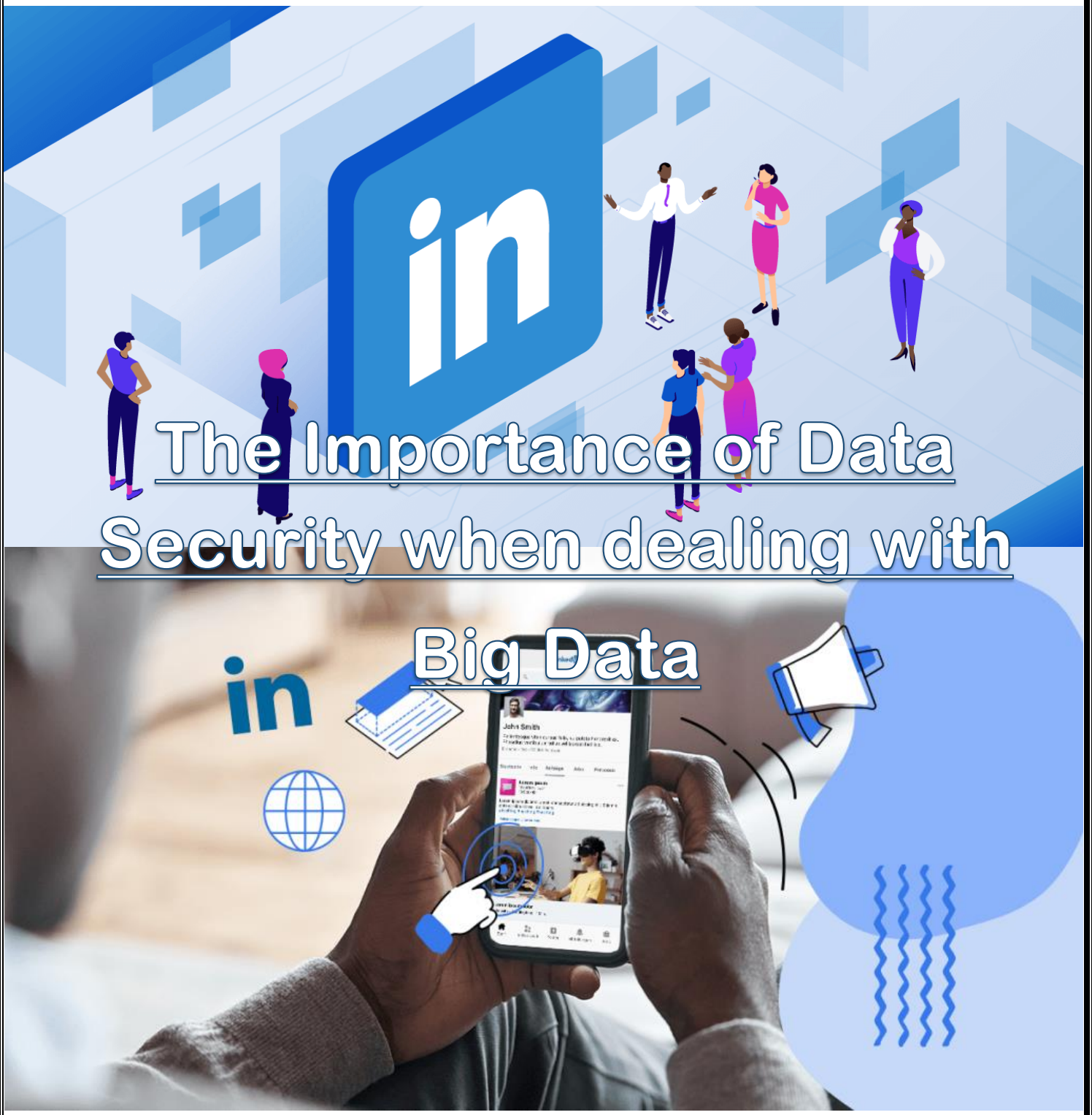

The Importance of Data Security when dealing with Big Data

Module: IS2184 Information System Management

Student No: 210458262

Word Count: 2435 words

Abstract

This essay focuses on Chapter 9 (Managing Business Intelligence and Big Data). It will mainly contain on Big data and Data Security by giving attention to the information systems issue which is “data breach”. This will be elaborated with a real life scenario of a data breach that happened with LinkedIn back in 2012. Lastly, critical reflections will contain an analysis of this issue under the topics of Strategic Planning and Morals, Ethics and Law which are based on Chapter 3 and 11.

Contents

1.Introduction and Context

1.1 Big Data

Big data refers to the huge, diverse information collections that are always expanding and for which conventional data management software is insufficient. The "three v's" of big data are information volume, velocity that is generated and collected, and variety of data points taken into account.

Big Data can be helpful to firms in many ways;

To better understand Where, When, and Why their consumers make purchases.

The company's supply chain can be made more efficient by identifying factors they could improve.

With the use of past and current data, it is possible to examine customer preferences, expectations and market situations which identifies and reduce the risks of an unforeseeable future incident.

The huge amount of data provides chances to research about new markets which are still not available enabling first mover advantage when starting up in a new market.

However, at the same time Big data will face certain challenges;

Data centers and databases used by businesses are constantly storing more data. When massive data sets grow quickly over time, managing them becomes more difficult.

When information is being gathered from many sources, problems with the quality of the data arise which impacts on the analysis. This is mainly from social media and fake URLs.

Keeping these data bases secure can be challenging since businesses typically put off data security because they are too busy studying their data sets. Hackers target data that isn't safeguarded.

1.2 Data Security

Protecting company and customer data and avoiding data loss due to unauthorized access is the process of data security. Businesses that want to adopt information security measures should follow the ISO 27001 principles provided by the International Organization for Standardization. These recommendations address subjects including access control, data storage, and encryption.

The 03 main elements of data security are;

- Data integrity indicates that there is no doubt that the data was not tampered with or degraded before or after submission.
- Confidentiality that indicates that the data is only accessible to authorized persons.
- Availability, which means that when needed, authorized individuals may access the company's information.

Data security in a firm is vital as they need to protect customer's privacy. Failing to do so will make them lose their customers to its competitors and go through lawsuits while losing its reputation.

Firms will find it challenging in securing big data, as increasing complexity of the computing environment every day will lead to an increase of potential entry points to a network which will increase the possibility of hackers to gain access to its data.

2.Information Systems Management Issue

2.1 Data Breach

Data Breaches faced by companies around the world can be seen as a serious problem as it affects both its customers and the firm itself. “A data breach is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals” (Reynolds et al., 2016).

Firms can face a Data Breach due to many ways such as;

A theft or loss of a physical object, such as a laptop, smartphone, USB drive, or external hard disk which will allow unauthorized access to sensitive data. Further, the information saved on the device can be easily accessed by the thief if it is not password secured or encrypted. This might lead to a significant disclosure of private information, such as financial or business secrets or personal information.

95% of cyber-security breaches, according to a research by IBM, are caused by human error. This is mainly due to weak passwords as many individuals rely on common words like "Password1" and "123456," which makes it simple for fraudsters to gain access to private data without any effort.

Malicious software can result in a data breach, where sensitive information gets leaked. It steals user credentials or even lock users out of their own systems. Hackers use this to gain unauthorized access to a company's network to extract valuable data such as customer information or trade secrets.

Insider leak can be more harmful because the insider already has access to the information and might not need to avoid security measures to get it.

A data breach might have extremely negative impacts such as;

The loss of customer confidence is one of the biggest long-term effects of a cybersecurity data breach. Consumers may trust businesses with their sensitive information since they have the required security measures in place to protect it. In a 2017 PwC study on customer views of cybersecurity and privacy risk, 92% of respondents said they thought firms should be proactive about protecting customer data.

Furthermore, firms will have to undergo financial losses. The longer the data breach remains undetected, the higher its financial impact as the remediation costs and loss of potential profits tends to be high.

Legal costs will be in millions as they will have to pay fines and penalties for not being able to protect information. But this will not end with paying fines but also after losing their brand reputation built all these years.

3.Discussion and Argument

3.1 Introduction to LinkedIn

LinkedIn is a social media platform designed specifically for professionals to connect and share information related to their industry or career interests.

With LinkedIn, users can create a professional profile that showcases their work experience, education, skills, and interests. The users can connect with other professionals in their industry, join groups and communities related to their field, and follow companies to keep updated on current events.

The LinkedIn app also offers job search and recruitment features, allowing users to search for job openings, apply for positions, and post job listings. It also helps companies and recruiters to find and hire qualified candidates. By the end of 2022, “LinkedIn has 875 million members, however it is not known how many are active every day or every month” (Iqbal, 2023).

3.2 Data Breach faced by LinkedIn

On June 5, 2012, a hacker gained access to LinkedIn, stealing the passwords for about 6.5 million user accounts. It was “not just stealing users’ passwords, but literally locking them out of their accounts” (SentinelOne, 2022). Over four years later in May 2016, a hacker going by the name "Peace" is selling a “database of 167 Million emails and hashed passwords, which included 117 Million already cracked passwords, belonging to LinkedIn users” (Kumar, 2016). Following this, LinkedIn officially announced that they were aware of the incident and have taken the required actions to reset the accounts that were thought to have been hacked.

One of the main reasons for LinkedIn to face this data breach was because they were not salting their passwords which enabled the hackers to crack its passwords easily. “According to LeakedSource, just 50 easily guessed passwords made up more than 2.2 million of the 117 million encrypted passwords exposed in the breach” (18 et al., 2016). Also, it was due to the lack of encryption used to protect user data. The stolen data was stored by LinkedIn in a format known as SHA-1, which is no longer considered a secure way.

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
11	000000	32,490
12	password1	30,981
13	abc123	30,398
14	charlie	28,049
15	linked	25,334
16	maggie	23,892
17	michael	23,075
18	666666	22,888
19	princess	22,122
20	123123	21,826

3.3 Analysis of this Data Breach

According to Reynolds (2016) one of the reasons why computer incidents are prevalent is due to Bring Your Own Device (BYOD) which is a policy that permits staff to access the company's computing resources and software using their own devices. The way LinkedIn's data reached to the hacker was when "the hacker found a LinkedIn employee who happened to also self-host his website" (Correa, 2021). Although the hacker found nothing of interest on that site, he also discovered another site being hosted on the same server; a WordPress site where he uploaded a malicious PHP script which enabled him access to LinkedIn.

Following can be seen as some efforts LinkedIn may have done to halt or lessen the danger of a data breach;

The firm could have assessed security-related risks and threats by undergoing risk assessment. This could have enabled LinkedIn to identify that not salting passwords and using SHA-1 for password protection was a serious threat as "SHA-1 was never meant to be used for password protection, but was actually designed for things like message authentication and data validation" (Correa, 2021) .

Moreover, LinkedIn can educate its employees and contract workers about the benefits of following safety policies such as applying strong passwords and strict access controls when obtaining any files from the device. This could have prevented data getting into hacker's hand.

Installing a corporate firewall, antivirus, and anti-spyware software and intrusion detection systems can help LinkedIn reduce its risk of a data breach. Since "LinkedIn did not find out about this hack until about 3 months later, when a hacker posted on a message board asking for help cracking passwords" (Correa, 2021) shows that they failed to lessen the effects by detecting immediately, creating a massive impact of millions of information getting leaked.

Here are some measures that LinkedIn took in response to the incident as well as some that they may have done;

They apologized for the incident and asked its customers to change the passwords immediately and invalidated the passwords of the accounts impacted, and contacted to reset their passwords.

They notified the relevant authorities (FBI) to trace the culprit Yevgeniy Nikulin and take legal action.

Moreover, they did an incident follow-up on how the security was compromised and made various security improvements to its platform, including implementing multi-factor authentication and using stronger encryption methods and salting its passwords.

4.Conclusion

Every day, businesses, organizations, and individuals create, store, and transmit vast amounts of data, ranging from financial information, confidential documents and sensitive government data. Therefore, in today's digital age when data keeps getting added and stored day by day it is important that it is protected from data breaches, and unauthorized access.

Since data cannot be easily retrieved again if faced with an attack, businesses should have backup to secure data in the event of a breach. Customers expect firms to react fast so that they will face a minimum damage. LinkedIn, however failed in this as users were disappointed on how long they took to handle the incident as it took days for password reset email to reach the user. Failing to gain customers trust will mean that the firm will lose out its customers, resulting in a revenue loss as well as facing lawsuits. LinkedIn had to pay up to $1.25 million to breach victims that paid a premium. In general, mitigating risks of a data breach will be cost effective for the firm by spending on securing data and research to improve data security than facing a sudden situation which costs millions of losses.

In general, no company will ever be totally safe from a breach. The key to preventing data security problems is to implement a comprehensive security system that makes computer break-ins difficult enough that an attacker eventually gives up. Companies must carry out routine IT security assessments as an act of prevention of data getting hacked.

5. Critical Reflections

5.1 Strategic Planning

Firms will have to make strategies where they will take specific actions to achieve its vision, mission, goals and objectives. When facing a problem such as a data breach, firms will have to make an issue based strategic planning approach. LinkedIn can identify the issue they are facing in current which is a data breach by analyzing its situation by making a SWOT analysis. Through this they can identify that the privacy breach is in fact a weakness as they had to spend $1.25 million to the victims and that privacy issues can be a threat because they cannot ensure that it will not happen again. Due to the 2012 data breach, LinkedIn failed to abide by its mission statement of their "commitment to be transparent about the data they collect and, how it is used and with whom it is shared" (2020). Therefore, LinkedIn will have to come up with strategies on how to reduce the negative impact of their weakness. Since a data breach is not always preventable they can implement a procedure to follow up in case of an emergency situation so that they can response quickly. They will also have to identify how they can defend against its threats of data breach to achieve LinkedIn's mission. Since prevention of a threat is better than curing it, they can come up with a proactive strategy rather than a reactive one. This can be done by undergoing regular audits which shows company's detailed examination of its security.

5.2 Morals, ethics and law

Morals relates to one's subjective beliefs about what is good and wrong, whereas ethics refers to the standard or standards of behavior required by the organization to which that individual belongs. Law is a collection of requirements for behavior that are imposed by a number of institutions (police, courts) which are mandatory to obey. Ethics should always come second in a firm's decision-making process, followed by the law. Yet, just because something is legal does not guarantee that it is likewise moral. When it comes to the LinkedIn data breach in 2012, there have been legal concerns as the company was hacked which invades legality.

Since it was a cracker (black hat) that got into the system with no permission for personal gains, where he sold sensitive information in the dark web and earned 5 bitcoins for each piece of information, the Russian hacker Yevgeniy Nikulin got imprisoned for 88 months.

Also, as LinkedIn failed to keep up with its privacy policies and user agreement they had to face with a class-action lawsuit where they had to pay $1.25 million to settle in. “The lawsuit charged LinkedIn with failing to meet its contractual obligations to protect users’ sensitive personally identifiable information (PII) with basic industry standard encryption methods” (Vaas et al., 2015). This can also be seen as unethical as it invaded privacy of their users which is not universally acceptable as any individual will not like their personal information to be available for the public to see.

6. Bibliography

18, J.F.M. *et al.* (2016) *As scope of 2012 breach expands, linkedin to again reset passwords for some users, Krebs on Security*. Available at: https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/ (Accessed: February 27, 2023).

Correa, C. (2021) *LinkedIn data breach 2012 case study*, *cecy*. Available at: https://www.cecy.dev/blog/linkedin-2012-breach-case-study/ (Accessed: February 27, 2023).

Iqbal, M. (2023) *LinkedIn usage and Revenue Statistics (2023), Business of Apps*. Available at: https://www.businessofapps.com/data/linkedin-statistics/ (Accessed: February 26, 2023).

Kumar, M. (2016) *Hacker puts up 167 million linkedin passwords for sale*, *The Hacker News*. Available at: https://thehackernews.com/2016/05/linkedin-account-hack.html (Accessed: February 27, 2023).

LinkedIn privacy policy (2020) *LinkedIn*. Available at: https://www.linkedin.com/legal/privacy-policy (Accessed: February 28, 2023).

Reynolds, G.W. (2016) "pg 31-59, 253-281, 301-382," in *Information Technology for managers*. Cengage Learning.

SentinelOne (2022) *Blast from the past: 2012 linkedin security breach dumps More than 100m additional records*, *SentinelOne*. Available at: https://www.sentinelone.com/blog/blast-past-2012-linkedin-breach-dumps-100m-additional-records/ (Accessed: February 27, 2023).

Vaas, L., Vaas, L. and Ducklin, P. (2015) *LinkedIn settles class action suit over 2012 unsalted password leak*, *Naked Security*. Available at: https://nakedsecurity.sophos.com/2015/02/25/linkedin-settles-class-action-suit-over-2012-unsalted-password-leak/ (Accessed: February 28, 2023).