LONDON METROPOLITAN UNIVERSITY

Module Code & Module Title

CC5052NP Professional Issues Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2nd Year, 2nd Semester

Student Name: Vamsha Palja Tamu

Group: L2C3

London Met ID: 21050019

College ID: NP04CP4A210106

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 content

1. Introduction

LinkedIn is a social media platform primarily used for professional networking and career development. It was founded in 2002 but was officially launched on May 5, 2003, and is headquartered in Sunnyvale, California. As of June 2021, the company reported over 740 million registered users in more than 200 countries worldwide. In December 2016, Microsoft completed its acquisition of LinkedIn, bringing together the world's leading professional cloud and the world's leading professional network (Linkedin, n.d.).

LinkedIn allows users to formulate a professional profile, connect with other professionals, and search for job opportunities. It is also a platform for sharing business-related content like articles and job postings. In addition, LinkedIn offers premium services for recruiters, marketers, and job seekers. These services encompass targeted job postings, interviewee tracking systems and advertising.

However, in June 2021, LinkedIn suffered a data breach, resulting in the disclosure of the personal information of over 700 million users. The leaked data included full names, email addresses, phone numbers, and other personal information. Although the company did not disclose the exact multitude of users affected, it urged all users to change their passwords and take other security measures to protect their accounts. The incident was a stark reminder of the importance of online security and the need for individuals and organizations to take proactive steps to protect their personal information.

2. Background on scandal

In June 2021, a major data breach occurred on the LinkedIn platform, resulting in the disclosure of the personal information of over 700 million users. Hackers were able to obtain LinkedIn users' personal information and put it up for sale on the dark web. This vulnerability affects 92% of the entire LinkedIn user base of 756 million users. The hackers released a sample of 1 million records to confirm the legitimacy of the breach, including email addresses, full names, phone numbers, geolocation records, LinkedIn usernames and profile URLs, personal and professional experiences, gender, and other social media accounts and details (Madeleine Hodson, privacysharks, 2021).

However, LinkedIn denied the data breach, arguing that the incident was just a violation of their Terms of Service through prohibited data scraping (Linkedin, 2023). According to LinkedIn, personal data was not compromised and the data was obtained from other sources as well (Linkedin, 2021). This incident raised several professional and social issues such as: the need for tighter security measures, the importance of data protection and the possible consequences of data breaches for individuals and organizations. LinkedIn users have been advised to take necessary security measures, such as: B. changing passwords and monitoring their personal information to protect against potential identity theft and fraud.

In addition, this data breach has also raised ethical concerns about the responsibility of social media platforms to protect their user data and the possible misuse of personal data for targeted advertising and other purposes. It underscores the need for organizations to prioritize data security and privacy, and the importance of transparency and accountability in data governance.

3. Legal issues

3.1. Lack of transparency

LinkedIn belatedly published the data breach that had happened as users' data was put up for sale on the dark web. Others only became aware of it and articles were published, after that only LinkedIn published about the data breach. LinkedIn should have should publicize the data breach as soon as it became known and allow informed users to take preventive action (civati, 2021).

3.2. Violation of data protection laws

The breach had violated privacy laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These laws oblige companies to take appropriate measures to protect personal data (e.g. assessing the risks associated with processing and measures to mitigate those risks, encryption) and to notify individuals in the event of a data breach (European Union, 2016) (California Legislature, 2020) but linkedin failed to maintain it due to the weak security of the company and the exposure of API to the third party that could collect personal information.

They need to have better security and have their API hidden well to prevent third party from seeing and finding it to exploit weakness.

3.3. Class action lawsuit

LinkedIn filed a lawsuit against a Singapore-based company alleging the scraping and sale of customer data after its data breach. There was settlement but no fine policy. Following to it, Linkedin had stated in a statement that it was not a data breach but a data scratch that includes publicly viewable member profile data that appears to have been scraped from LinkedIn. (Spicer & Edwards , 2022).

3.4. Government investigations

After the data breach, the Guarantor for the Protection of Personal Data (GPDP) launched an investigation against LinkedIn. after the breach of social networking systems led to the dissemination of user data, including IDs, full names, email addresses, phone numbers and links to others LinkedIn and other social media profiles, job titles and other job information entered by users into their profiles. Also considering that Italy is one of the European countries with the most subscribers to the platform, the Authority had reminds all users affected by the breach to pay particular attention in the coming weeks to any anomalies related to their phone number and account (Garante per la protezione dei dati personali, 2021) which is legal.

3.5. Violation of personal Privacy and failure to protect it

Due to the data breach on LinkedIn, the valuable information of users that had a mixture of both private and public information such as full names, LinkedIn profile names, LinkedIn IDs, LinkedIn profile URLs, gender, email addresses, phone numbers, physical addresses, geolocation records, industry information, personal experience, and professional experience (Isbitski, 2021). As such pieces of information were exposed to the public by the hacker, it violated the personnel privacy of users and it also meant that the company LinkedIn was unable to protect it.

4. Social issues

4.1. Weak password

When a combination of numbers and a variety of characters, as well as the type of information associated with the secret word Is an obvious sequence that may occur multiple times, a password could be categorised as a weak password. eg 123456, 123456789, etc. After a data leak, even if the hacker cannot obtain the victim's password, they may have access to other sensitive data, such as birth dates, social security numbers and addresses, which may make the job of deciphering password easier (incognia, n.d.). For that, victims and all others should have a strong password, difficult to be guessed easily because of its length with all sorts of characters and numbers.

4.2. Cyber Attacks

Due to the sensitive information of the victims of the data breach being collected by the hacker, could make targeted phishing attacks could be sent to the victims by spamming emails and phone numbers in them (Cybernews Team, 2023). Nevertheless, a normal person, not technologically literate, will not find the attacks suspicious and will fall for them and further harm themselves. The solution is to educate the masses on technology.

4.3. Damage to professional reputation

as previously stated, LinkedIn is a professional network to find jobs. users of LinkedIn are basely there for professional networking and job opportunities searching. Users of LinkedIn are basely there for professional networking and job opportunities searching. The stolen information could be used by a third party to impersonate users, send phishing emails or post false information, resulting in confusion and mistrust among colleagues, potential employers and interviewees (Johansen, 2021).

4.4. Identity theft

Typically, the likelihood of identity theft is high among victims due to data breaches. Hackers or any person who purchases the information either can use the stolen information to open credit accounts, make fraudulent purchases, or commit other crimes that may have a long-lasting effect on victims, including financial loss, damaged credit, and emotional distress (Jennifer van der Kleut for NortonLifeLock, 2021). The user can check whether their information has been leaked or not at specific websites.

4.5. Loss of trust

Building trust is difficult. it is even more difficult to build with unknown strangers. Due to the loss of the personnel information of victims in the aftermath of LinkedIn data breach, the user of LinkedIn could have lost trust which was hard built as they were not able to protect the personnel of their information. It may be obvious that the company could rebuild the trust of the customer if the company does not let data breaches occur in the first place, give the customer more control over their data, have a security person or firm as a partner, etc (sia innovations, n.d.).

5. Ethical issues

5.1. Impersonation

As mentioned above, as a victim may possess a weak password, the hacker could gain access to the victim's account and impersonate the victim in order to send phishing emails or send false information to scams, causing confusion and distrust among those connected to them (Jennifer van der Kleut for NortonLifeLock, 2021). The user should have been able to establish a more difficult, secure and unique password. After gaining access to victims' accounts, hackers can use them as they choose, resulting in hackers only seeing their profit and not caring about other factors that might have a long-lasting effect on the victim.

5.2. Risk on right and freedom of individual

In situations where a data breach poses a high risk to those individuals affected then they should all be informed, unless effective technical and organisational protection measures have been put in place or other measures that ensure that the risk is no longer likely to materialise (european commission, n.d.). LinkedIn should have notified them of the data breach immediately to the user that was exposed in data breach and they should have appropriate measures to secure it.

5.3. Social engineering and networking

Social engineering involves the manipulation of human error to gain valuable private information (DAS, 2021). Hackers exploit social engineering to extract valuable information by gaining information on an account or network of people. The hacker could be accessing your account with publicly available information (name, dates, email, geolocations/address) from the data breach to impersonate you to gain access to your network.

5.4. Negligence in responsibility

LinkedIn's vulnerability in the security of the platform led to negligence in the security of the platform as they had exposed their API which made data scraping easier. LinkedIn had stated that it was a data scrape, it violated their terms and services and they work to stop them and punish those who are responsible. The statement also proved that they do not want to be responsible for the data scrap from its site and its constant falling to improve the security of its API (Wille, 2021).

5.5. Notifying supervisory authority about data breach

In case the breach occurred without undue delay, and where possible, the controller of personal data (company) should have informed the supervisory authority about the data breach within 72 h from the time they were aware of it and unless the breach of personal data is unlikely to result in a risk to the rights and freedoms of natural persons (EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016). We do not have information on whether LinkedIn has informed the supervisory authority but looking at the graveness of the situation, it could have risks to the victim's rights and freedom such as cyber attacks, phishing, scams, etc leaving a long-lasting effect.

6. Professional issues

6.1. Damage to professional health

In a survey conducted by ThreatConnect, 500 IT professionals from USA and UK were selected, and it was founded that the professionals are also affected by the data breach as 27% suffer from high-stress levels, and 27 had their lifestyle changes due to over-work and forced to be available all time , the health care system is susceptible to be on deterioration because of mental pressure.

6.2. Week API

Because LinkedIn had a weak API that caused it to be abused by third parties to gain access to millions of users' personal information. Misuse of this API opens up potential security risks for many people and companies using LinkedIn (scrubbed, n.d.). LinkedIn should have made its API strong from the start to make it harder to scrap around the web and hide it from other third-party libraries. others should not have been able to see all sensitive information and only vague information and information that they wanted to show.

6.3. Security vulnerability

According to the internal investigation, LinkedIn had improper security configurations that left user data exposed to unauthorized access due to improperly configured access tokens which allowed hackers gain access to user data (Wille, 2021). LinkedIn had failed to improve its API as it had previously occurred which makes it unable to withstand a data breach.

6.4. Lack of immediate action

LinkedIn was too late to take immediate action as they were still unsure about the data breach and delayed verifying the data breach information until June 29, but the data was sold on a form from June 22. Privacy Sharks had contacted LinkedIn and what they responded with was that in their analysis, they identified that the scrapped information from LinkedIn was not only from LinkedIn but also from other places, and no private data was leaked and also violated their terms and conditions (Hodson, 2021). LinkedIn than verified the data after the information became public.

6.5. Failed to protect and respect personal privacy

As stated previously, LinkedIn had their user data collected and also from other places, which proved that LinkedIn was unable to uphold the statement that they take the safety and security of our members' accounts seriously (Linkedin, 2016). They were unable to take into account necessary measures that protect the safety and security of the users to respect and protect the personnel privacy of users as leaked data contained user's full names, LinkedIn profile names, LinkedIn IDs, LinkedIn profile URLs, gender, email addresses, phone numbers, physical addresses, geolocation records, industry information, personal experience, and professional experience (Isbitski, 2021).

7. Conclusion

The case study on the LinkedIn data breach 2021 June 21 was completed with extensive research, dedication, and effort. The purpose of this case study was to investigate the different types of issues that arose after the LinkedIn data breach, such as legal issues, ethical issues, social issues and professional issues. On 22 June 2021, LinkedIn suffered from a data breach which exposed critical and valuable information of 700 million users as a sale in a dark web forum.

LinkedIn responded to the media by saying it was not a data breach but a data scrape. It was morally wrong as stated in the theory of Deontology because the company repeatedly attempted to deny it was a data breach.
after the data breach had been publicized on a hacker forum, LinkedIn should have contacted the proper authority and the victims of the data breach within 72 hours of knowing it but they neglected to inform anybody which makes it their fault for not informing the user to take measures to secure their account and because they were unable to hold and protect their user properly and their data securely. As the same method was used in this case and previously which was API vulnerability stated, LinkedIn had also been doing Negligence in securing the platform from any possible vulnerability. The security of LinkedIn should have been improved, learning from previous experiences, and it should continue to improve but unfortunately, it didn't. LinkedIn should take appropriate measures to protect their users as their information was leaked leaving them vulnerable to other parties. Also, LinkedIn was late to announce the cause of the data breach, as it was on 29 June and when it was released they stated that they were still investigating the data breach. A big corporation must have an immediate response team and security team, that they take over in any kind of incident and one which purely focuses on the security of the platform to further secure it from attack.

The users of LinkedIn or any other online platform should use a strong password that is not easily guessed to ensure that on an occasion of a data leak or breach, they are not compromised because their personal information was leaked. The user should also be vigilant so that they do not use the same password repeatedly and keep their ears open to know about any type of data breach and

leaks. The users should know what constitutes a scam and phishing attack to prevent their failure. The users should also take available protective measures to further secure their account such as two-factor authentication (2FA), etc.

The government and others should spread knowledge to any users about their presence on the internet, how to beware of any third party that might seek to cause harm to them and how to beware of any type of scam and cyber attacks.

From this case study, I gained the importance of what ethics should a person have and why one should have ethics to further develop selves and have morals that define them as a human. it has been a pleasure to do this case study as it contributed to my self-development in research and analytical skills for further refining the content that fits the requirements of what I wanted. Despite the difficulties, it was overcome with hardship leaving me with grand perceptiveness and great wisdom.

8. Bibliography

Anon., n.d.

California Legislature, 2020. *Civil Code § 1798.150.* [Online] Available at: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.150

[Accessed 18 03 2021].

civati, A., 2021. *2021 Data Breaches - A brief Review.* [Online] Available at: https://www.linkedin.com/pulse/2021-data-breaches-brief-review-alessandro-civati

[Accessed 19 03 2023].

Cybernews Team, 2023. *Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof.* [Online] Available at: https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

[Accessed 26 03 2023].

DAS, A., 2021. *Hacking Humans: 5 Ways You Can Be Exploited on Social Media.* [Online] Available at: https://www.makeuseof.com/social-media-used-for-human-hacking/

[Accessed 26 03 2013].

european commission, n.d. *What is a data breach and what do we have to do in case of a data breach?.* [Online] Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en#:~:text=If%20that%20occurs%2C%20and%20it,become%20aware%20of%20the%20breach.

[Accessed 25 03 2023].

EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016. Notification of a personal data breach to the supervisory authority. *General Data Protection Regulation.*

European Union, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.* [Online]

Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[Accessed 20 03 2021].

Garante per la protezione dei dati personali, 2021. *LinkedIn: after the data theft, the Guarantor opens an investigation on the social network and warns that the use of data deriving from the violation is illegal. Users advised to pay particular attention to possible anomalies on their mobile phones or acc.* [Online]
Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9573647#fromHistory
[Accessed 20 03 2023].

Hodson, M., 2021. *Exclusive: 700 Million LinkedIn Records For Sale on Hacker Forum, June 22nd 2021*. [Online]
Available at: https://www.privacysharks.com/exclusive-700-million-linkedin-records-for-sale-on-hacker-forum-june-22nd-2021/
[Accessed 21 03 2023].

incognia, n.d. *What makes a password weak?*. [Online]
Available at: https://www.incognia.com/the-authentication-reference/what-makes-a-password-weak
[Accessed 25 03 2023].

Isbitski, M., 2021. *Recap: The 7 Biggest API Security Incidents in 2021*. [Online]
Available at: https://salt.security/blog/recap-7-biggest-api-security-incidents-in-2021
[Accessed 25 03 2023].

Jennifer van der Kleut for NortonLifeLock, 2021. *Identity theft: What is it and how to avoid it.* [Online]
Available at: https://us.norton.com/blog/id-theft/what-is-identity-theft#:~:text=Identity%20theft%20is%20one%20of,sale%20on%20the%20dark%20web.
[Accessed 22 03 2023].

Johansen, A. G., 2021. *4 Lasting Effects of Identity Theft.* [Online]
Available at: https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft
[Accessed 23 03 2023].

Linkedin, 2016. *Protecting Our Members.* [Online] Available at: https://blog.linkedin.com/2016/05/18/protecting-our-members [Accessed 25 30 2023].

Linkedin, 2021. *An update on report of scraped data.* [Online] Available at: https://news.linkedin.com/2021/april/an-update-from-linkedin [Accessed 21 3 2021].

Linkedin, 2023. *Prohibited Software and Extensions.* [Online] Available at: https://www.linkedin.com/help/linkedin/answer/a1341387/prohibited-software-and-extensions?src=re-other&veh=www.privacysharks.com%7Cre-other [Accessed 21 3 2023].

Linkedin, n.d. *About linkedin.* [Online] Available at: https://about.linkedin.com/ [Accessed 21 03 2023].

Madeleine Hodson, privacysharks, 2021. *Exclusive: 700 Million LinkedIn Records For Sale on Hacker Forum, June 22nd 2021.* [Online] Available at: https://www.privacysharks.com/exclusive-700-million-linkedin-records-for-sale-on-hacker-forum-june-22nd-2021/ [Accessed 21 3 2023].

Marcia Ernst, 2016. *Data Breaches.* [Online] Available at: https://www.sgrlaw.com/ttl-articles/data-breaches/#:~:text=Data%20breach%20lawsuits&text=Plaintiffs%20typically%20seek%20damages%20for,to%20investigate%2C%20and%20emotional%20distress. [Accessed 20 03 2023].

scrubbed, n.d. *LinkedIn Data Leak – What We Can Do About It.* [Online] Available at: https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/ [Accessed 21 03 2023].

sia innovations, n.d. *Loss Of Trust: A Cybersecurity Attack's Invisible Consequence.* [Online] Available at: https://www.siainnovations.com/blog/loss-of-trust-a-cybersecurity-attacks-invisible-consequence/#:~:text=Loss%20of%20customer%20trust%20adds,and%20lower%20your%20co

mpany's%20value.
[Accessed 27 03 2023].
Spicer, c. & Edwards , J., 2022. *LinkedIn Data Breach Lawsuit Settled By Barring Singapore-Based Scraper.* [Online]
Available at: https://topclassactions.com/lawsuit-settlements/privacy/data-breach/linkedin-data-breach-reportedly-exposes-personal-salary-info-of-700m-users/
[Accessed 18 03 2023].
Wille, M., 2021. *Hackers used LinkedIn's official API to leak tons of data... again.* [Online]
Available at: https://www.inverse.com/input/culture/hackers-used-linkedins-official-api-to-leak-tons-of-dataagain
[Accessed 25 30 2023].