LinkedIn Data Breach Research

: Katyani Bajgain Chhetri

Table of Contents

1. Introduction 1

2. Background of the Scandal 3

3. Legal Issues 6

4. Social Issues 8

5. Ethical Issues 10

6. Professional Issues 12

7. Personal Reflection 14

Bibliography 16

Table of Figures

Figure 1: LinkedIn Logo (LinkedIn, n.d.)..... 1

Figure 2: Hacker's message (Taylor, 2021) 3

Figure 3: Information of the users in the sample provided by the hacker (Taylor, 2021). 4

Figure 4: Text with the hacker (Taylor, 2021) 5

1. Introduction

A social networking website is a website that provides a social community for people interested in a particular subject. Social networking website can be defined as a web-based service which allows individual to construct a public or a semi-public profile within a bounded system, communicate with other users; view the pages and the details provided by other users within the system. Some examples of social networking website include Facebook, Instagram, LinkedIn etc. LinkedIn is one of the most used social networking websites. (Ahmad, 2011)

LinkedIn began in co-founder Reid Hoffman's living room in 2002 and was officially launched on May 5, 2003. LinkedIn is the world's largest professional network. You can use LinkedIn to find the right job or internship, connect and strengthen professional relationships, and earn the skills you need to succeed in your career. You can access LinkedIn from a desktop, LinkedIn mobile app, mobile web experience, or the LinkedIn Lite Android mobile app. (LinkedIn, 2023)

Figure 1: LinkedIn Logo (LinkedIn, n.d.)

With more than 45 million users representing 150 industries around the world, LinkedIn is a fast-growing professional networking site that allows members to create business contacts, search for jobs, and find potential clients, Individuals have the ability to create their own professional profile that can be viewed by others in their network, and also view the profiles of their own contacts. (Dukaric, 2009)

Today, LinkedIn leads a diversified business with revenues from membership subscription, advertising sales and recruitment solutions under the leadership of Rayan Rolanksy. In December

2016, Microsoft completed its acquisitions of LinkedIn, bringing together the world's leading professional cloud and the world's leading professional network. (LinkedIn, 2023)

The one simple mission of LinkedIn is to connect the world's professionals to make them more productive and successful. A complete LinkedIn profile can help you connect with opportunities by highlighting your unique professional story through experience, skills, and education. (LinkedIn, 2023)

2. Background of the Scandal

On June 22, 2021, a user of a popular hacker forum (Raid Forums) advertised data of 700 LinkedIn users containing information of their LinkedIn profile for sale after 500 million LinkedIn enthusiasts were affected in a data scrapping incident previously in April. The alleged hacker posted a sample of the data that included the data of 1 million, LinkedIn users. The samples when examined revealed that it to contained information such as:

- Email Addresses
- Full Names
- Phone numbers
- Geolocation records
- LinkedIn username and profile URL
- Personal and professional experience/background
- Other social media accounts and usernames (Taylor, 2021)

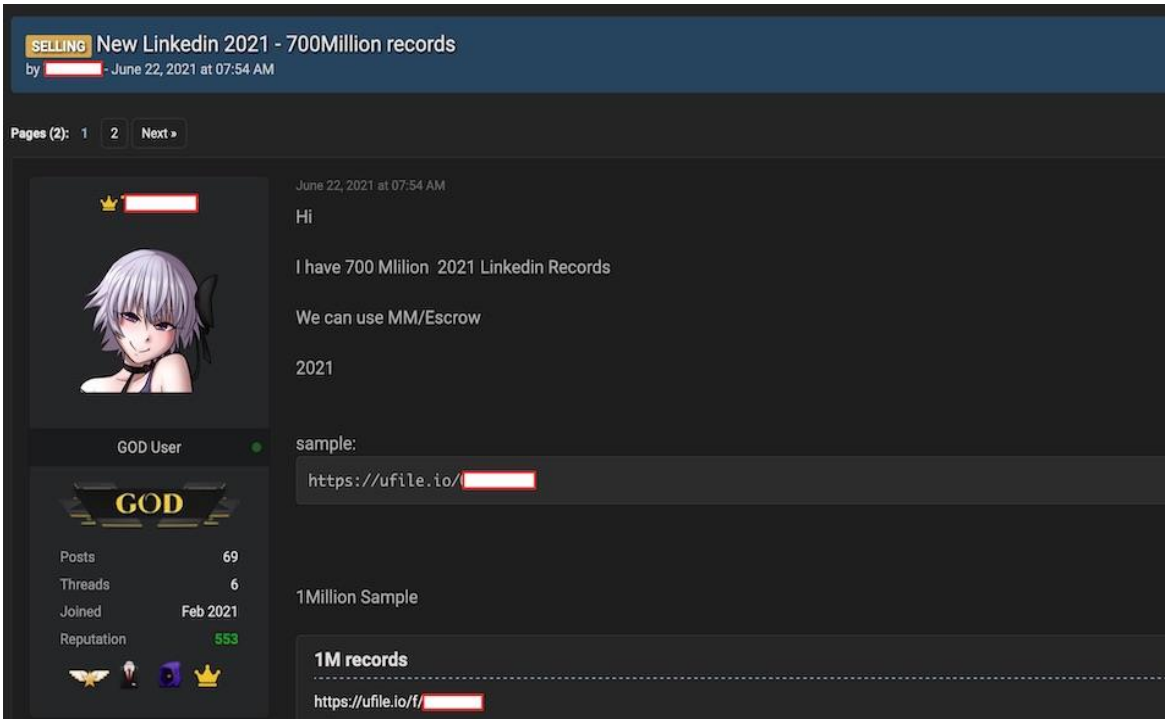

Figure 2: Hacker's message (Taylor, 2021)

The hacker allegedly claimed that the complete database contained the information of 700 million users. Since LinkedIn has 756 million users it meant that 92% of all LinkedIn users could be found in the records. As it can be observed from the above presented picture that a sample of the acquired records was provided by the hacker. Upon examination the information that was present in the sample were authentic and tied to the real users based on analysis and cross checking of the data from the sample with other publicly available information. (Taylor, 2021)

Figure 3: Information of the users in the sample provided by the hacker (Taylor, 2021).

As per the source the hacker claimed that the information was obtained by exploiting the LinkedIn API to harvest the information that the users uploaded to their website (Taylor, 2021) . The LinkedIn API [Application Programming Interface] was misused by a third-party to gain access to the personal data of millions of users. The misuse of this API opened potential security risks for many people and companies who use LinkedIn as their primary platform for business connections. (John, et al., n.d.)

After the leak occurred LinkedIn made an official statement claiming that it was the case of data scrapping and data aggregation from different sources and that it was not a data breach. The official Statement – "We want to be clear that this is not a data breach, and no private LinkedIn member data was exposed. Our initial investigation has found that this data was scraped from

LinkedIn and other various websites and includes the same data reported earlier this year in our April 2021 scrapping update". (LinkedIn, 2021)

The hacker allegedly caused the breach to acquire LinkedIn user's information to offer it up for sale. The hacker asked for $5000 for the data set. The below presented picture is the conversation with the hacker regarding the data breach and the sale of the user's information as per Restore Privacy (Taylor, 2021).

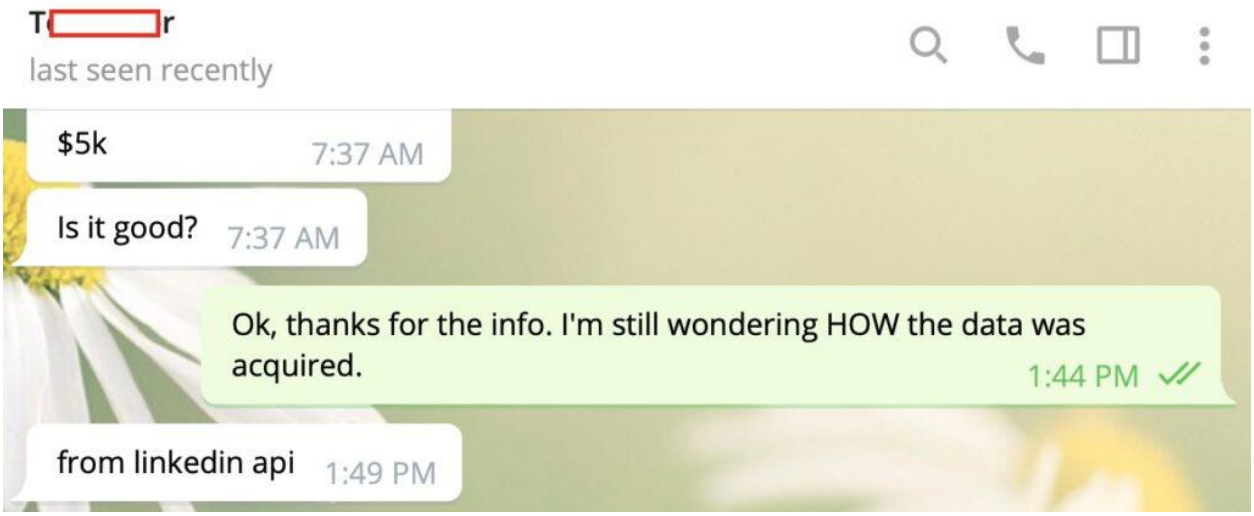

Figure 4: Text with the hacker (Taylor, 2021)

3. Legal Issues

LinkedIn in violated many of the rules and regulations as per the law in the June 22, 2021, data breach incident. Some of the legal issues that occurred in that incident are presented below:

- **Failed to meet the security claims as per the LinkedIn Data Processing Agreement(LDPA):** LinkedIn failed to meet the security claims as per the LinkedIn Data Processing Agreement because LinkedIn clearly states in the LDPA that appropriate organizational and technical security measures will be maintained to protect against unauthorized or accidental access, loss, incident response, encryption of Customer Personal Data while in transit and at rest, alteration, disclosure, or destruction of customer Personal Data. (LinkedIn, 2022) but as per the resources the breach occurred due to the misuse of the LinkedIn API via a third party to gain access of the personal data of users and post it up for sale without the knowledge of the users. Thus, LinkedIn did not abide by the LinkedIn Data Processing Agreement. General breach of contracts/agreements could also result to reduction in contract price, remedy of the defect, compensation for damage and interest for delay (Virtual Lawyer, n.d.)

- **Violation of GDPR regulation:** The article (34) of GDPR is "Communication of a personal data breach to the data subject" and the article states that "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay and in timely manner" (intersoft consulting, n.d.) but the law was violated by LinkedIn as they only released an official statement in June 29, 7 complete days after the breach happened [June 22] and the users information was on the dark web without the users being aware or even notified, the violation of the GDPR regulation could result to a fine of up to 10 million dollars and if an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher (intersoft consulting , n.d.).

- **Violation of California Consumer Privacy Act:** CCPA provides a right to "limit use and disclosure of sensitive personal information for consumer which states that a consumer/user can direct businesses to only use your sensitive personal information for limited purposes, such as providing with services that are requested (CCPA, 2023)." As the personal information of

the users was accessed by a third party from an organization [LinkedIn] for foul purposes and was put out for sale in the dark web without the users consent or their knowledge, the third party [hackers] could be fined up to $2500 per violation and $7500 each for intentional violations (Clarip, n.d.).

- **Violation of Computer Fraud and abuse act**: The computer fraud and abuse act prohibit intentionally accessing a computer without authorization or more than authorization. It has become a tool ripe for abuse and use against nearly every aspect of computer activity (NACDL, n.d.). Thus, any sort of hacking activity is going against the CFAA and so does the hacking regarding the linked in data breach. The consequence of the violation of this act can be prison sentence from 1 year to even 10 years (NACDL, n.d.).

- **Violation of the personal information protection and Electronic Documents Act (PIPEDA)**: Under this act there is a regulation "Breach of Security Safeguard Regulations" it is required for the concerned organization to notify the affected individual with the description of the circumstances of the breach, the date and time of occurrence, and the extent of data compromised (laws-lois, 2018). Since linked only posted a statement stating the incident and denying all the accusations and not mentioning any of the information above thus the act was violated by LinkedIn. The consequence for the violation of this act could be a fine up to $100,000 (HUsain, 2023)

4. Social Issues

Since LinkedIn is a social networking website it connects people into an online society. The breach that occurred on June 21, 2021, gave rise to a list of social issues listed as below:

- **Loss of trust:** LinkedIn claimed to protect the data provided by the users in the licensed agreement between the users and LinkedIn (LinkedIn, 2022). But the obtaining of data [user information] by an unauthorized party and the data being up for sale in the dark web proved it otherwise which will cause the users to lose trust in LinkedIn. And the trust in Microsoft [owner of LinkedIn] and its services has been impacted as well (Jhonson, 2021). The social networking world is built on trust. Since there is so much sensitive customer data involved, part of that trust means guaranteeing data safety (SIA innovations, n.d.). These types of incidents would make the users lose trust not only with the concerned organization - LinkedIn but also any other social networking platforms and question their ability in protecting the user's personal data.

- **Reputational Damage:** A successful data breach involving the loss of customer data could put the brands reputation on the line. Breach victims can easily share their experiences over social media and news outlets causing a PR nightmare for the organization. Data breaches get a lot of bad press and even misinformation getting added on the incidents which causes a lot of damage on the organization's reputation itself and any other brands/organizations linked with it (SIA innovations, n.d.). This type of reputational damage could lead LinkedIn to loss of tremendous revenue, goodwill, and most of all the customers[users].

- **Risk of cyberattacks:** After the linked in data breach the user information was put up on the dark web for sale by the hackers. (Taylor, 2021). With details such as email addresses and phone numbers made available to the buyers online, individuals could become a target of identity theft, spam campaigns. Sensitive data can be tracked down just with email information by expert hackers. Linked in users could also be receiving end of email or telephone scams that tick them into sharing sensitive credentials or transferring large amount of money (Hodson, 2021). The emails provided for sale on the dark web could be used by the hackers to make many attempts to access users accounts using various combination making the user a victim of brute force attacks (Hodson, 2021)

- **Loss of control with personal information:** Once details have been posted to the dark web, they stay there forever. It's not a question of one buyer attains the rights to the data and they get taken down, anyone who wants them can pay the fee and have access to the data (west, 2019). This can result to the clients feeling distressed about their information being out everywhere and not knowing about where their information being used. This also means that the users are prone to getting hacked as long as the information is out on the dark web for the hackers to buy.
- **Psychological Impact:** With the personal information being everywhere the users are at peak risk of being a victim of cyber-attacks such as hacking and scams. The stolen personal information can be spread rapidly intensifying the feelings of helplessness leading to anxiety and also feeling demoralized. The emotional and psychological impact following the losses related to cybercrime can range from mild to severe and lead to symptoms of depression, anxiety, panic attacks, and posttraumatic stress. The invasion to one's privacy that results from cyber-attacks also translate into grief (Katy Kamkar, 2021). Thus, these sorts of breaching incidents causing personal data leak can have a heavy psychological impact on the victims.

5. Ethical Issues

The LinkedIn data breach was ethically wrong in several different ways as the incident runs against all the ethical theories. The description on how the incident was ethically wrong is presented below:

- **Violation of virtue theory:** The virtue theory emphasizes on merits or moral character rather than one's duties or rules of consequences of actions (Baase, 2012). it takes the person's morals, reputation, and motivation into account when rating an unusual and irregular behavior that is considered unethical (Chonko, n.d.). The virtue theory was violated by the hackers by engaging in activities that are dishonest, unfair, disrespectful, and irresponsible, which are immoral and unethical according to the principles of virtue theory. Also, on LinkedIn's part they are morally obligated to protect the personal data of the user which they have failed to deliver multiple times.

- **Violation of Deontological theory:** Deontology is an ethical theory that uses rules to distinguish right from wrong (Baase). The deontological class of ethical theories states that people should adhere to their obligations and duties when engaged in decision making when ethics are in play (Chonko, n.d.). Hackers violate the deontological theory by engaging in activities that violate principles such as respect for property, honesty which are immoral and unethical according to the principles of deontological theory. Also, LinkedIn went against the deontological theory by going against the rule of securing the personal data provided by the users.

- **Violation of utilitarianism:** Utilitarianism is based on one's ability to predict the consequences of an action (Baase, 2012). To a utilitarian, the choice that yields the greatest benefit to the most people is the one that is ethically correct (Chonko, n.d.). Hackers go against utilitarianism by causing harm to a large people through their actions. Utilitarianism aims to maximize overall happiness and minimize overall suffering for greatest number of people. LinkedIn also acted against utilitarianism as the company failed to adequately protect the personal data of its users. The breach caused harm to many people, which runs counter to the rule utilitarianism which goes against the law (Chonko, n.d.)

- **Violation of Rights:** Rights is established by society and given the highest priority and considered to be ethically valid since a large population endorses them (Baase, 2012). One of the negative rights as per "Rights" is right to privacy and with the data breach the right to privacy of the users have been hindered as their information had been extracted without consent and been put up for sale on the dark web. This incident is a clear breach to right to privacy of the LinkedIn's users, as right to privacy being a fundamental human right which includes the right to control one's personal information and data to prevent it from being disclosed to others without one's consent.

6. Professional Issues

The linked in data breach was unprofessional in the hacker's part as well as LinkedIn's part. Some of the professional issues of the respective incident is listed below:

- **Misuse of knowledge:** Exploiting digital systems and networks through unauthorized access to any account or computer is a typical explanation of hacking. A lone renegade programmer who is extremely competent in coding and changing computer software systems is the typical image of a hacker (Narang, 2023). The misuse of knowledge occurs when someone uses their knowledge or skills for unethical or illegal purposes. Therefore, hacking Is often considered a misuse of knowledge because it involves using technical expertise for illegal or unethical purposes, which causes harm to other.

- **Lack of accountability:** An organization should strive to notify users about a data breach as soon as possible and take steps to mitigate the impact of the breach as it is the organizations are accountable towards the users. The LinkedIn data breach happened on June 22, 2021, but LinkedIn only posted an official statement after 7 business days denying the breach (LinkedIn, 2021) with no warning, preventive measures, or compensation of any sort to the users. This showed lack of accountability for LinkedIn. LinkedIn response to the breach was very underwhelming with the slow notification process and lack of transparency regarding the extent of the data that was compromised.

- **Negligence with Data Security:** In 2012 6.5 million LinkedIn accounts had been compromised and again in 2016 117 million users' data was put up for sale including the users' usernames and password (spring, 2016). Again, in June 2021 April 500 million data from LinkedIn was retrieved and again In June 700 million users' data was extracted and put on the dark web for sale (Taylor, 2021). Such ongoing pattern of the data breaches along the years compromising the personal data of the users shows severe negligence and weakness of LinkedIn in implementing adequate security measures.

- **Overpromising and Underdelivering:** In the agreement between the users and LinkedIn (LDPA) LinkedIn claims to protect the personal information of the users and the website free from external fraud and abuse (LinkedIn, 2022) which is overpromising to the

customers because the continuous course of data breaches and data leak of the personal information of more than 700 million users is considered underdelivering and even deceiving. Such actions prove to be very unprofessional on LinkedIn's part.

- **Disrespecting Confidentiality:** As a computer professional it is their responsibility to understand privacy and the rights and responsibilities associated with the collection of personal use (Baase, 2012). Hackers use various forms of cyberattacks to gain unauthorized access to personal and sensitive data. Thus, by illegally accessing and misusing personal information the hackers defy their responsibility as a computer professional.

7. Personal Reflection

In the LinkedIn data Leak scandal of 2021, the personal information of more than 93% of LinkedIn users was put on sale on the dark web by hackers. The hackers provided a sample of personal information of 1 million of the LinkedIn's user which comprised of information such as email address, Full name, phone numbers, geolocation records, LinkedIn username and profile URL, personal experience, genders, and other social media accounts and details. The information was allegedly obtained by exploiting LinkedIn's API.

The most pressing issue of this incident is the unauthorized access to the personal information of the users. This greatly affects the users whose data were compromised and the organization itself. The compromised personal data and the lack of responsibility of LinkedIn in this incident the major concerns of the scandal. This not only brought threat to the user with consequences such as the risk of getting hacked, identity theft, psychological impact it also greatly impacted the organization with the consequences such as reputation damage, loss of trust with users. The sole motive behind the incident seems to be money as the personal information of the users was put up for sale by the hackers. Such type of data breaches can be avoided only if the organizations comply with the mitigating preventive such as improving the security protocols, fixing security vulnerabilities, preparing a safety course of action in case of a breach.

LinkedIn could have easily avoided the breach of June 22, 2021, as there has been multiple different breaches of same sort in the past. LinkedIn could have examined the previous breaches identified the root cause and complied with the preventive measure such as conducting regular security assessments and vulnerability scans to identify and address the potential security weaknesses, organize regular training and awareness programs for employees to ensure data security, use strong encryption to protect sensitive data and use a strong firewall to block any sort of unauthorized access. Since the data breach wasn't avoided and the right of the user such as right to privacy got violated Linked has responsibilities to the users such as upholding professional ethics, being transparent and accountable for the breach and take actions immediately to further stop such incidents.

In conclusion LinkedIn being such a large organization need to be more focused towards the security of the personal data entrusted to them by the users. Such negligence in repetitive course

of action can cause linked in to face loss in customers as well as revenue. The entire social networking world is built on trust and LinkedIn being such a great part of it must take necessary actions and prevent any further breaches from happening.

Bibliography

Ahmad, A., 2011. *A short description of social networking websites and its uses.* [Online]
Available at: https://www.researchgate.net/publication/50235019_A_Short_Description_of_Social_Networking_Websites_And_Its_Uses
[Accessed 28 April 2023].

Baase, S., 2012. *A Gift of Fire: Social, legal and ethical issues fro computing and the internet alternative etext formats.* 4th ed. s.l.:Prentice Hall.

CCPA, 2023. *Califronia COnsumer Privacy Act.* [Online]
Available at: https://oag.ca.gov/privacy/ccpa#:~:text=Right%20to%20limit%20use%20and,such%20as%20providing%20you%20with
[Accessed 16 April 2023].

Chonko, L., n.d. *dsef.org.* [Online]
Available at: https://dsef.org/wp-content/uploads/2012/07/EthicalTheories.pdf
[Accessed 23 april 2023].

Clarip, n.d. *Clarity in Privacy.* [Online]
Available at: https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/#:~:text=Intentional%20violations%20of%20the%20California,violations%20is%20%242500%20per%20violation.
[Accessed 16 April 2023].

Collins, K., 2023. *Secure Ideas.* [Online]
Available at: https://www.secureideas.com/knowledge/what-risks-does-the-darkweb-pose-to-businesses
[Accessed 22 April 2023].

Dukaric, R., 2009. *linkedIn:Onlin community research,* s.l.: https://people.eng.unimelb.edu.au/vkostakos/courses/socialweb10F/projects/2009.linkedin.paper.pdf.

Hodson, M., 2021. *privacy Sharks.* [Online]
Available at: https://www.privacysharks.com/exclusive-700-million-linkedin-records-for-sale-on-hacker-forum-june-22nd-2021/
[Accessed 22 April 2023].

HUsain, O., 2023. *Penalties for Noncompliance With PIPEDA & How Its Enforced.* [Online]
Available at: https://www.enzuzo.com/blog/pipeda-penalties-enforcement#:~:text=Penalties%20for%20PIPEDA%20Noncompliance,-If%20your%20organization&text=At%20this%20time%2C%20businesses%20and,is

%20aggressive%20in%20its%20investigations.
[Accessed 30 April 2023].

intersoft consulting , n.d. *intersoft consulting.* [Online]
Available at: https://gdpr-info.eu/issues/fines-penalties/#:~:text=For%20especially%20severe%20violations%2C%20listed,fiscal%20year%2C%20whichever%20is%20higher.
[Accessed 15 April 2023].

intersoft consulting, n.d. *Art.32 GDPR.* [Online]
Available at: https://gdpr-info.eu/art-34-gdpr/
[Accessed 15 April 2023].

Jhonson, t., 2021. *omdia.* [Online]
Available at: https://omdia.tech.informa.com/blogs/2021/what-are-the-implications-of-linkedins-latest-data-breach
[Accessed 22 april 2023].

Jhonson, T., 2021. *What are the implications of LinkedIn's latest data breach?,* s.l.: informa.

John, Chester & Nicko, n.d. *scrubbed.net.* [Online]
Available at: https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/
[Accessed 11 April 2023].

Katy Kamkar, R. D., 2021. *thesafetymag.* [Online]
Available at: https://www.thesafetymag.com/ca/news/opinion/psychological-trauma-and-cybercrime/252447
[Accessed 28 April 2023].

laws-lois, 2018. *laws-lois.justice.gc.ca.* [Online]
Available at: https://laws-lois.justice.gc.ca/PDF/SOR-2018-64.pdf
[Accessed 30 April 2023].

LinkedIn, 2021. *LinkedIn Pressroom.* [Online]
Available at: https://news.linkedin.com/2021/june/an-update-from-linkedin
[Accessed 11 April 2023].

LinkedIn, 2022. *LinkedIn Data Processing Agreemnet.* [Online]
Available at: https://www.linkedin.com/legal/l/dpa
[Accessed 15 april 2023].

LinkedIn, 2023. *LinkedIn.* [Online]
Available at: https://www.linkedin.com/help/linkedin/answer/a548441/what-is-linkedin-and-how-can-i-use-it-?lang=en#:~:text=LinkedIn%20is%20the%20world's%20largest,to%20succeed%20in%20your%20career.
[Accessed 31 March 2023].

LinkedIn, n.d. *LinkedIn Brand.* [Online]
Available at: https://brand.linkedin.com/downloads
[Accessed 31 March 2023].

NACDL, n.d. *nacdl.org.* [Online]
Available at: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct
[Accessed 30 April 2023].

Narang, M., 2023. *knowlwdgehut.* [Online]
Available at: https://www.knowledgehut.com/blog/security/ethical-hacking-vs-hacking
[Accessed 22 April 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/
[Accessed 22 April 2023].

spring, t., 2016. *threat post.* [Online]
Available at: https://threatpost.com/2012-linkedin-breach-just-got-a-lot-worse-117-million-new-logins-for-sale/118173/
[Accessed 22 April 2023].

Taylor, S., 2021. *New LinkedIn Data leak leaves 700 million users exposed.* s.l.:Restore Privacy.

United Nations, n.d. *universal Declaration of HUamn Right.* [Online]
Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks.
[Accessed 16 April 2023].

Virtual Lawyer, n.d. *consequences of breach of contract in general.* [Online]
Available at: https://virtuallawyer.fondia.com/en/articles/consequences-of-breach-of-contract-in-general#:~:text=The%20common%20consequence%20is%20reduction,making%20a%20contract%20or%20separately
[Accessed 23 April 2023].

west, F., 2019. *LinkedIn.* [Online]
Available at: https://www.linkedin.com/pulse/dark-web-what-cost-you-ignore-francis-west/
[Accessed 22 april 2023].