

Abstract

The 2021 LinkedIn data breach exposed the personal and professional information of millions of users globally, having consequences on the law, ethics, and society. This paper includes an overview of the LinkedIn data breach, its causes, effects, and potential consequences for users and society.

The report examines the incident's causes and analyses it. The breach's wider consequences, including the need for data privacy and security, are also covered, highlighting how crucial it is for people, businesses, and governments to take preventative action to stop and lessen the effects of cyberattacks. This report also consists of personal reflection and summary about the whole incident and includes suggestion in order to emphasize the importance of the LinkedIn data breach in the current digital era and the need for ongoing efforts to ensure data privacy and security.

Table of Contents

1. Introduction	1
2. Background	2
2.1. Cause	2
2.2. Impact.....	3
3. Legal Issues	5
3.1. General Data Protection Regulation (GDPR)	5
3.2. California Consumer Privacy Act (CCPA)	6
3.3. UK Data Protection Act 2018	6
3.4. Australian Privacy Act 1988	7
3.5. Brazilian General Data Protection Law (LGPD)	7
4. Social Issues	7
4.1. Social Distrust	7
4.2. Privacy Concerns.....	7
4.3. Awareness and Education	8
4.4. Data Ownership and Control.....	8
4.5. Importance of Protecting users data.....	9
5. Ethical Issues	9
5.1. Transparency and Accountability.....	9
5.2. Potential Harm.....	9
5.3. Data Protection Regulation	9
5.4. Proper Communication	9
5.5. Individual Shared Responsibility	10
6. Professional Issues	11

6.1. Reputational Damage	11
6.2. Professional Relationship.....	11
6.3. Economic Burden.....	11
6.4. Competitive Disadvantage	12
6.5. Litigation Risks	12
7. Personal Reflection.....	13
8. References	14

Table of Figures

Figure 1 LinkedIn's office at US (Lunden, 2019).....	1
Figure 2 Healthcare Data Breaches Statistics over the years (The HIPAA Journal, 2023).....	2
Figure 3 LinkedIn's Leaked Database on sale in Telegram (Cybernews Team, 2023).	3
Figure 4 LinkedIn Users' Leaked Data (Taylor, 2021).....	4
Figure 5 LinkedIn Posts about the incident (LinkedIn Corporate Communications, 2021).....	5
Figure 6 Consumer Awareness of Data Breaches Chart (Security.org Team, 2022).	8

1. Introduction

In today's digital landscape, the threat of cyber-attacks is ever-present and can impact both individuals and organizations. The responsibility of safeguarding sensitive data can be overwhelming, and it is essential for users to remain vigilant at all times. With many organizations becoming victims of data breaches and student and official accounts being exposed, it is crucial to take measures to address this issue (Ravi Teja Kamurthi, 2021).



Figure 1 LinkedIn's office at US (Lunden, 2019).

LinkedIn is the world's largest professional social network with more than 900 million members in more than 200 countries and territories worldwide which was officially launched on May 5, 2003 (LinkedIn Corporation, 2023).

LinkedIn is an online social media platform that helps individuals from diverse backgrounds like entrepreneurs, learners, and jobseekers to advance their careers (LinkedIn Corporate Communications, 2021). It provides access to a network of professionals, groups, and organizations that can offer assistance and support in their respective fields.

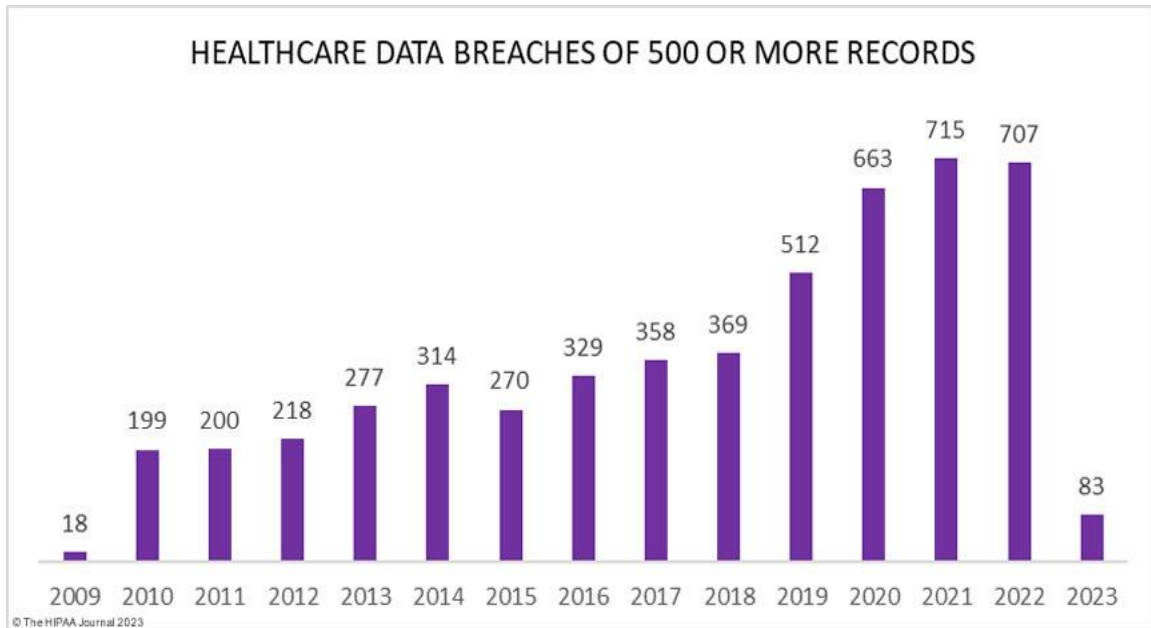


Figure 2 Healthcare Data Breaches Statistics over the years (The HIPAA Journal, 2023).

In recent years, not just tech companies such as Facebook, Twitter, LinkedIn have faced data breach incidents. But even Healthcare and other various industries have been affected by data breach and other cyber-attacks. The above image shows the recent statistics over the years in the HealthCare sector which seem to have been growing tremendously each year.

2. Background

LinkedIn which is a popular professional social networking site among the people around the world seeking to connect with each other grow their professional network and connect with like-minded people faced it's yet another data breach in June 2021.

A database of information with data on over 700 million LinkedIn users was leaked online after hackers attempted to sell it earlier this year (Cimpanu, 2021). The Record obtained the data from a source, and it is currently being circulated in private Telegram channels and Dark Web Forums as an archived torrent file, totalling around 187 GB.

2.1. Cause

A third party gained access to millions of LinkedIn user's personal data by misusing LinkedIn's API, which creates security risks for users and companies. LinkedIn had taken steps to resolve the issue and claimed the data leak resulted from data aggregation

from various sources, including publicly viewable member profile data, rather than a data breach (Scrubbed, 2021). They asserted that no private member data were exposed.

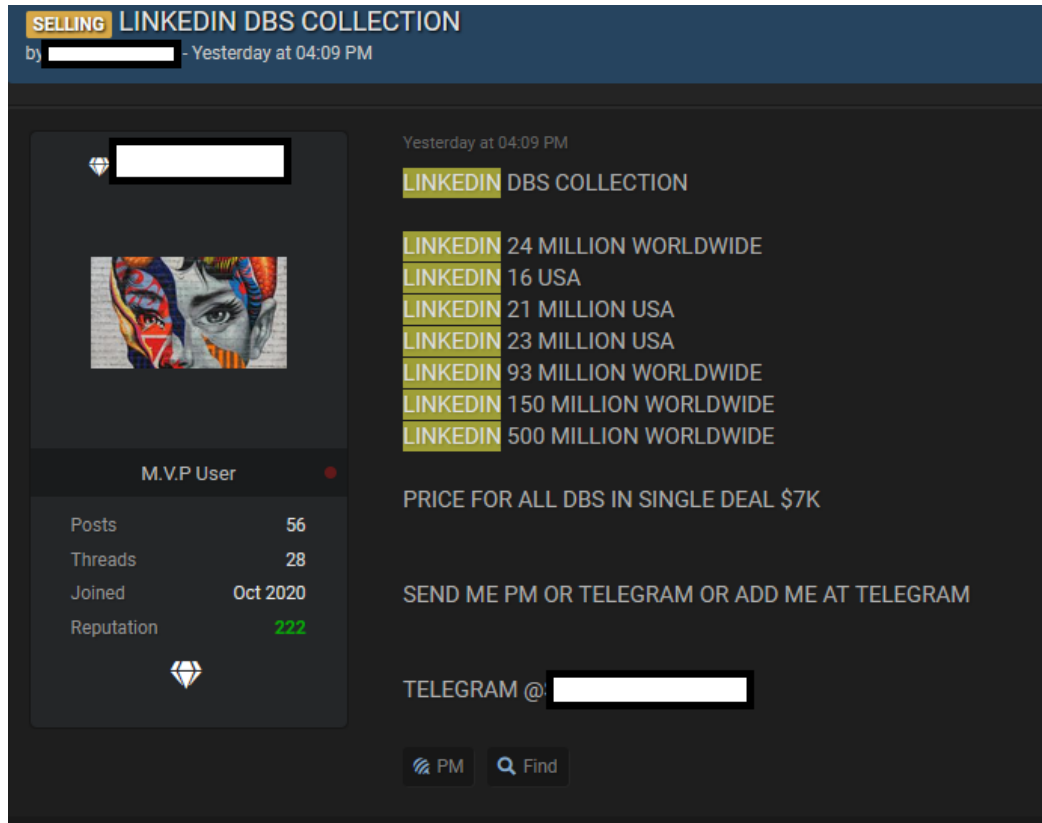


Figure 3 LinkedIn's Leaked Database on sale in Telegram (Cybernews Team, 2023).

Various sources were found to have been selling the users personal information and data over 500 million in different platforms in which one of them was Telegram as you can see in the image above.

2.2. Impact

In a sample of one million entries from a collection of data believed to be scraped from LinkedIn, email addresses, full names, phone numbers, physical addresses, geo-location records, LinkedIn user profiles, personal and professional backgrounds, gender, and social media account usernames were found (Scrubbed, 2021). No passwords or credit card information was exposed. Users are warned of the increased risk of social engineering attacks, as the leaked contact details can be used in phishing and identity theft attacks (Scrubbed, 2021). Hackers can use the information from LinkedIn accounts, along with information from other platforms such as Facebook and Twitter, to create fake LinkedIn accounts or access other accounts.

```

"full_name":"charlie [REDACTED]","gender":"male",
"linkedin.com/[REDACTED]5",
"linkedin_username":"charlie-[REDACTED]5","linkedin_id":"2[REDACTED]3",
"facebook_url":"facebook.com/v[REDACTED]",
"facebook_username":"v[REDACTED]",
"facebook_id":"1[REDACTED]5",
"work_email":"c[REDACTED].com",
"mobile_phone":"+15[REDACTED]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts"
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01",
"linkedin_connections":120,"inferred_salary":"[REDACTED]",
"inferred_years_experience":5,
"summary":"I am a moti[REDACTED]"
"full_name":"mehari [REDACTED]"
"linkedin_url":"linkedin.com/[REDACTED]",
"linkedin_username":"mehari-[REDACTED]5",

```


Figure 4 LinkedIn Users' Leaked Data (Taylor, 2021).

Hackers may have used the compromised data for unethical purposes like identity theft, financial fraud, and phishing attacks. Users have suffered reputational harm as a result of the breach since their business information may have been made public. LinkedIn had urged users to secure their accounts by changing their passwords and turning on two-factor authentication as a result of the breach (Scrubbed, 2021). Users must be careful and take the appropriate security measures to protect their personal and professional information.

LinkedIn has faced serious concerns regarding customer security in the wake of two data breaches that occurred within the past years. These breaches impacted a massive number of users, which has prompted LinkedIn to overhaul their security policies. During the second breach i.e. June 2021, Cyber Criminals were able to extract users' full names, email addresses, phone numbers, and physical addresses from the site (Brandon Gibson, 2021). This type of sensitive information can be used by malicious actors for a variety of nefarious purposes, making it critical for LinkedIn and its users to take swift and decisive action.

An update on report of scraped data

Published on Jun 29, 2021 | Categories: [Product News](#)

 LinkedIn Corporate Communications



Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. 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 scraping update](#).

Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.

For additional information about our policies and how we protect member data from misuse: <https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions>

Figure 5 LinkedIn Posts about the incident (LinkedIn Corporate Communications, 2021).

The LinkedIn 2021 data breach was quite large in scale and scope because sensitive personal and professional information from millions of users around the world were included in the compromised data. Users were therefore advised to exercise caution and keep a close eye on their online accounts for any indications of unusual activity. By updating their **passwords**, enabling **two-factor authentication**, and avoiding clicking on **dubious links or emails**, they should also take precautions to secure their accounts.

3. Legal Issues

The breach had exposed users' sensitive personal and professional information, including names, email addresses, phone numbers, and physical addresses. Legal issues related to the LinkedIn data breach was significant, as the incident had violated various data protection and privacy laws.

3.1. General Data Protection Regulation (GDPR)

GDPR is a strict privacy and security law that applies to any organization that targets or collects data related to people in the EU. It took effect on May 25, 2018, and imposes harsh fines for violations, reaching into the tens of millions of euros (Proton AG, 2023).

The LinkedIn data breach of 2021 possibly breached GDPR, which mandates organizations to protect personal data and notify affected individuals and regulators promptly in case of a data breach. Under the GDPR, LinkedIn could have faced a maximum fine of up to **€20 million or 4%** of their annual global turnover (whichever is higher) for violating the regulation. The exact amount of the fine would depend on various factors such as the nature, gravity, and duration of the breach, the number of affected individuals, the measures taken by the company to mitigate the damage, and the level of cooperation with authorities.

3.2. California Consumer Privacy Act (CCPA)

The CCPA of 2018 empowers Californian consumers with rights to control personal information collected by businesses, including the right to know, delete, opt-out, and non-discrimination for exercising these rights (Rob Bonta, 2023).

The LinkedIn data breach of 2021 had violated the California Consumer Privacy Act (CCPA), which requires businesses to implement appropriate data security measures and mandates prompt notification of affected individuals and regulators in case of a data breach. The exposure of personal and professional information of Californian users could be considered a breach of CCPA, and LinkedIn could have faced **legal consequences and financial penalties** as well if found negligent in protecting user data and failing to comply with CCPA requirements. Under the CCPA, LinkedIn could have got the penalty up to **\$7500 per violation**.

3.3. UK Data Protection Act 2018

The LinkedIn data breach of 2021 violated the UK's Data Protection Act 2018 by exposing users' personal and sensitive information without their consent and failing to implement adequate security measures. This breaches the act's data protection principles, including **fair use, accuracy, and appropriate security measures**, which regulate how organizations use personal information (gov.uk, 2023). Under the UK Data Protection Act 2018, the potential punishments could have included fines of up to **€20 million or 4%** of the company's global annual revenue. The Act also provides for other penalties, such as legal action by affected individuals and reputational damage to the company.

3.4. Australian Privacy Act 1988

The LinkedIn data breach of 2021 also violated the Privacy Act 1988, the main Australian law governing personal information handling, by exposing personal data without consent or adequate security measures, thus breaching privacy principles (Australian Government, 2023). Under the Act, companies are required to take reasonable steps to protect personal information from misuse, interference, and loss, as well as unauthorized access, modification, or disclosure which LinkedIn was found not have secured.

3.5. Brazilian General Data Protection Law (LGPD)

The Brazilian General Data Protection Law (LGPD) permits the processing of personal data by individuals or entities, public or private, for the protection of **fundamental rights of privacy and free development of personality** (iapp, 2020). The LinkedIn data breach of 2021 also violated the LGPD by exposing personal data of Brazilian users without their consent, breaching the law's requirements for explicit consent, appropriate security measures, and prompt notification of data breaches to affected individuals and authorities as LinkedIn has its users all around the globe.

4. Social Issues

The breach had significant impact on the society as the users' data were found be leaked and sold in multiple forums and platforms. This incident must have resulted in a lot of social issues such as:

4.1. Social Distrust

The data breach may have also contributed to a growing sense of distrust and concern among users about the safety and security of their personal information online. Many people rely on social networking platforms like LinkedIn to connect with friends, family, and colleagues, and to share personal and professional information.

4.2. Privacy Concerns

The breach may have eroded users' trust in these **platforms and reduced their willingness to share** personal information online, which could have negative impacts on social media usage and engagement.

4.3. Awareness and Education

The social issues associated with the LinkedIn data breach underscore the need for greater awareness, education, and transparency regarding the risks of cybercrime and data protection. Greater awareness of data breaches and how the consumers can mitigate their own personal risk of information leak can be one of the main mitigations for data breaches as well.

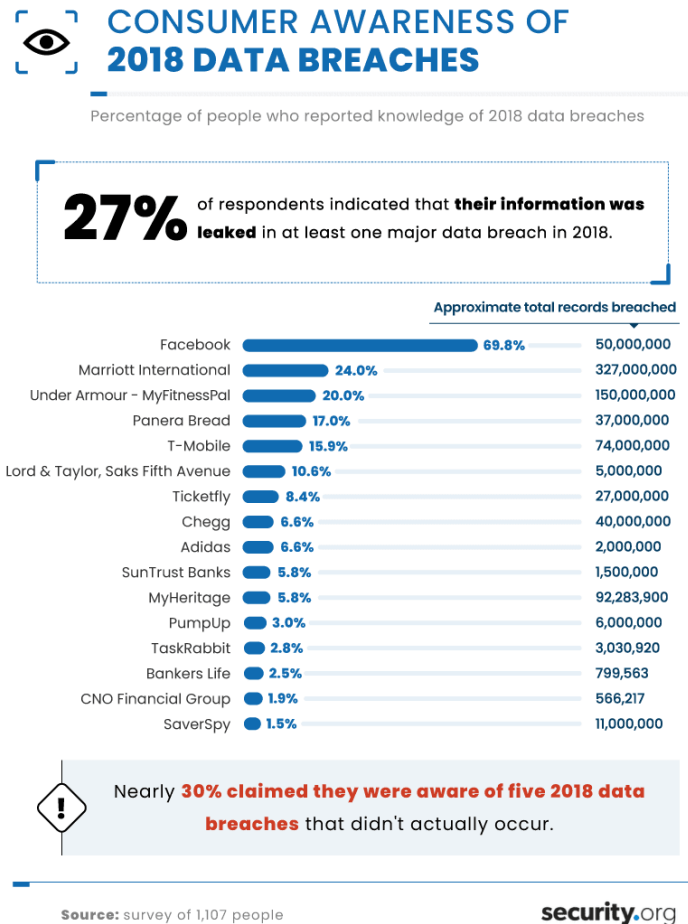


Figure 6 Consumer Awareness of Data Breaches Chart (Security.org Team, 2022).

4.4. Data Ownership and Control

The breach highlighted the issue of data ownership and control. Many users of social media platforms may not be aware of the extent to which their personal information are being collected and used by companies. The breach also gained concerns about how companies collect and use personal data and highlighted the need for greater transparency and accountability in the data collection and usage practices of social media platforms.

4.5. Importance of Protecting users data

The breach also raised the importance of protecting user data and the ethical responsibility of companies to ensure that user data is adequately protected. The incident may have eroded users' trust in social media platforms, which could have **negative social implications** for the future of online communication and social media engagement.

5. Ethical Issues

Every company has to follow a proper code of conduct to handle incidents such as data breaches. LinkedIn had caused multiple ethical issues in which some of them have been listed below.

5.1. Transparency and Accountability

Companies have an ethical responsibility to protect its users data and ensure that users privacy is adequately safeguarded. The breach clearly shows the need for greater **transparency and accountability in the data collection and usage practices** to ensure that users' personal information is protected (Raval, 2022).

5.2. Potential Harm

The exposure of personal and professional information could have resulted in identity theft, financial fraud, or other forms of harm to users. LinkedIn should have promptly notified affected users about the breach and provided them with resources to protect their personal information within 72 hours if it were to follow GDPR.

5.3. Data Protection Regulation

The data breach could have been prevented with better data protection regulation. LinkedIn could have collaborated with policymakers to build **stronger data protection regulations** to ensure users' information. However, they failed to do which resulted to have been the cause of the data breach.

5.4. Proper Communication

In the European Union, the General Data Protection Regulation (GDPR) requires organizations to notify the appropriate supervisory authority within **72 hours** of becoming aware of a data breach (Satori Cyber, 2023). And, for breaches unlikely to

result in a risk to the rights and freedoms of individuals, reporting to the supervisory authority is not required. Organizations also required to notify individuals without undue delay if the data breach is likely to result in a high risk to their rights and freedoms (Satori Cyber, 2023).

Hence, LinkedIn could have established clear lines of communication with affected users and provided them with a way to report any suspicious activity related to the breach and should keep things transparent to regain its reputation as soon as the breach occurred. The company should have also worked with law enforcement agencies to identify and prosecute those responsible for the breach.

5.5. Individual Shared Responsibility

While companies have an ethical responsibility to protect user data, individuals also have a role to play in safeguarding their personal information. This includes individuals to be aware of the risks of cybercrime and taking steps to protect sensitive information, such as using **strong passwords** and being cautious about **sharing personal information** online.

6. Professional Issues

Data breach incidents can have negative impact for both the consumer and the company in the professional market. LinkedIn's data breach which took place on June 2021 could have caused a lot of professional issues for LinkedIn itself and its users as well. Some of the issues that may have been invoked by the breach are:

6.1. Reputational Damage

According to the Ponemon Institute, "Businesses that experienced less than a **2% loss of customers** had an average loss of **\$2.67 million in sales**, while companies that lost more than **5% of their customers** faced an average revenue loss of **\$3.94 million**. The study also found that the stock values of companies tend to decrease by an average of 5% after a data breach becomes public (Raval, 2022)."

In the case of LinkedIn, the personal and professional information leak, including job titles, email addresses, and other sensitive information, could also have a range of negative consequences for individuals, such as reputational damage or the risk of identity theft and could have lost numbers of users as well.

6.2. Professional Relationship

The breach may also have impacted users' employment prospects or professional relationships. For example, if a user's personal or professional information was compromised, it could lead to embarrassment or loss of trust among colleagues or potential employers. This in turn, could have long-lasting effects on users' career prospects or opportunities.

6.3. Economic Burden

According to the IBM Cost of a Data Breach 2022 Report, the average cost of data breach is said to be increased 2.6% from **\$4.24 million in 2021** to **\$4.35 million in 2022** (Reed, 2022). The breach also undermined the credibility of LinkedIn as a professional networking platform. LinkedIn users rely on the platform to connect with colleagues, expand their professional networks, and showcase their expertise. The breach in turn could have negative consequences for LinkedIn's user base and revenue.

6.4. Competitive Disadvantage

A data breach resulted in the exposure of confidential information of the users, this allowed and opened attack surface for hackers seeking to extort various things and perform illegal activities. This incident could erode LinkedIn's competitive advantage in the market, potentially leading to a loss of market share and revenue.

6.5. Litigation Risks

According to **Norton Rose Fulbright's latest Annual Litigation Trends Survey** of more than 250 general counsel and in-house litigation practitioners, cybersecurity and data protection will be among the top drivers of new legal disputes for the next several years (Hill, 2022). Two-thirds of survey respondents said they felt more exposed to these types of disputes in 2021, up from less than half in 2020, while more sophisticated attacks, less oversight of employees/contractors in remote environments, and concerns about the amount of client data were all cited as mitigating factors (Hill, 2022). Hence, data breaches can lead to class-action lawsuits, particularly if large numbers of users are affected which can lead to significant legal costs and reputational damage for the company.

7. Personal Reflection

The one of the largest LinkedIn's data breach which took place on June 2021 and many other data breaches before and after has demonstrated the proper need for heightened data security measures in recent years. The incident had exposed the vulnerability of user data and highlighted the potential risks associated with inadequate security protocols. It is crucial for individuals, organizations, and governments to work together to prevent similar breaches from happening again in the future.

The LinkedIn data breach serves as a stark reminder of the **importance of data privacy and security** in the modern world and highlights why all organizations and companies should prioritize customer's data and evaluate and remediate the consequences the issues they might create.

The root causes of the data breach such as human error, software vulnerabilities, and cyber-attacks, must be thoroughly examined and addressed to prevent similar breaches in the future. Companies and individuals should prioritize **regular security awareness**, audits and assessments, as well as stay **vigilant and proactive** about potential security risks in a regular basis without any hesitation.

Hence, it is crucial for individuals, organizations, and governments to take proactive measures to protect sensitive information, as cyber-attacks are becoming increasingly sophisticated and prevalent. By working together, the companies can strengthen their defences and protect against future data breaches, ensuring the safety and security of our digital lives by following proper cyber security guidelines, policies and compliance.

8. References

Security.org Team. (2022, December 20). Public Awareness of Major Data Breaches. Retrieved from <https://www.security.org/resources/data-breach-awareness/>

Australian Government. (2023). Rights and Protection. Retrieved from <https://www.ag.gov.au/rights-and-protections/privacy>

Brandon Gibson, S. T. (2021). Vulnerability in Massive API Scraping: 2021. Oxford: International Conference on Computational Science and Computational Intelligence (CSCI).

Cimpanu, C. (2021, September 22). Hackers leak LinkedIn 700 million data scrape. Retrieved from The Record: <https://therecord.media/hackers-leak-linkedin-700-million-data-scrape>

Cybernews Team. (2023, February 20). Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof. Retrieved from <https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/>

gov.uk. (2023). The Data Protection Act. Retrieved from <https://www.gov.uk/data-protection>

Hill, M. (2022, April 19). Cybersecurity litigation risks: 4 top concerns for CISOs. Retrieved from <https://www.csoonline.com/article/3656700/cybersecurity-litigation-risks-on-the-rise-what-cisos-should-worry-about-the-most.html>

iapp. (2020, October). Brazilian General Data Protection Law (LGPD, English translation). Retrieved from <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/>

LinkedIn Corporate Communications. (2021, June 29). An update on report of scraped data. Retrieved from <https://news.linkedin.com/2021/june/an-update-from-linkedin>

LinkedIn Corporation. (2023). LinkedIn. Retrieved from About LinkedIn: <https://about.linkedin.com/>

Lunden, I. (2019, February 12). TechCrunch. Retrieved from LinkedIn debuts LinkedIn Live, a new live video broadcast service: <https://techcrunch.com/2019/02/11/linkedin-debuts-linkedin-live-a-new-live-video-broadcast-service/>

Proton AG. (2023). What is GDPR, the EU's new data protection law? Retrieved from GDPR.EU: <https://gdpr.eu/what-is-gdpr/>

Raval, K. (2022, January 11). How Can Data Breaches Affect Brand and Reputation. Retrieved from <https://martechvibe.com/martech/how-data-breaches-can-affect-brand-and-reputation/>

Ravi Teja Kamurthi, S. R. (2021). Confrontation- Wi-Fi Risks and Data Breach. Pune: International Conference on Emerging Smart Computing and Informatics (ESCI).

Reed, J. (2022, October 13). How Do Data Breaches Impact Economic Instability? Retrieved from <https://securityintelligence.com/articles/how-data-breaches-impact-economic-instability/>

Rob Bonta. (2023, April 24). California Consumer Privacy Act (CCPA). Retrieved from <https://oag.ca.gov/privacy/ccpa>

Satori Cyber. (2023, February 28). Communication of Data Breach: Repairing Your Reputation and Staying Compliant. Retrieved from <https://satoricyber.com/data-privacy/communication-of-data-breach>

Scrubbed. (2021, July 21). LinkedIn Data Leak – What We Can Do About It. Retrieved from <https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/>

Taylor, S. (2021, June 27). New LinkedIn Data Leak Leaves 700 Million Users Exposed. Retrieved from Restore Privacy: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/>

The HIPAA Journal. (2023). Retrieved from Healthcare Data Breach Statistics: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

