

Case Report

Open Access

A Case Study: Data Breaches on Latitude Financial Services

Fereshteh-Azadi Parand ^{1*}, Sara Tavakoligolpaygani ²

1. Department of Statistics, Mathematics, and Computer Science, Allameh Tabataba'i University, Tehran, Iran.

2. Faculty of Science and Engineering, Macquarie University, Sydney, Australia.

Abstract

One of the most effective methods in the field of cyber-security is the study of attacks and their causes. This paper examines the cyber-attack on Latitude Financial in March 2023, which exposed critical vulnerabilities within Australia's digital infrastructure and compromised the personal data of millions. It investigates the attack's methodology, uncovering insider involvement and misconfigured security settings as key enablers. The study highlights the significance of unpatched software and weak passwords in exacerbating system vulnerabilities, emphasizing the imperative for robust cyber-security measures.

The breach's impact on customers underscores privacy and trust concerns, necessitating stricter regulations and improved security protocols. The analysis of attack methods underscores the evolving cyber threat landscape, urging proactive defence strategies. Moreover, the breach highlights the importance of comprehensive cyber-security measures, including employee training and stringent access controls.

The paper advocates for regulatory reforms to enforce data security standards and ensure accountability among organizations and service providers. It explores the potential of cyber insurance in mitigating post-attack burdens, emphasizing the need for policy enhancements and addressing coverage gaps.

Ultimately, the Latitude Financial breach underscores the urgency for comprehensive reforms in data security practices and regulatory frameworks. By prioritizing consumer data protection, companies and regulatory bodies can mitigate risks and uphold trust in an increasingly digitized world.

Keywords Data Breaches, Cyberattack, Cyber Insurance, Security

1. Introduction

The cyberattack on Latitude Financial Services in March 2023 marked one of the most significant data breaches in Australia's history, affecting customers, past customers, and applicants across Australia and New Zealand. The breach exposed sensitive personal information, including nearly 8 million driver's license numbers, over 50,000 passport numbers, and more than 6 million customer records. In examining this breach, several crucial topics

emerge. Firstly, understanding the method employed in the attack sheds light on the perpetrators' tactics. Secondly, identifying the vulnerabilities exploited in the system(s) provides insights into the weaknesses that allowed such a breach to occur. Thirdly, establishing accountability and motivations behind targeting Latitude Financial is essential for understanding the broader context of the incident. Additionally, assessing potential preventive measures is crucial for mitigating future risks. Furthermore,



© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

* Correspondence:
parand@atu.ac.ir

exploring the role of Cyber Insurance in alleviating such risks can provide valuable insights into risk management strategies. Finally, observing the repercussions experienced by customers in the aftermath of the breach offers valuable lessons for both affected individuals and organizations striving to enhance their cybersecurity posture [1][2]

Method Employed in the Attack

In the realm of cyber warfare, attackers employ a myriad of tactics to breach systems, compromise data, and wreak havoc on organizations. Common methods of cyberattacks include malware, denial of service (DoS) and distributed denial of service (DDoS) attacks, SQL injection, cross-site scripting (XSS), man-in-the-middle (MitM) attacks, brute force attacks, social engineering, and phishing. Each of these methods exploits different vulnerabilities in systems, applications, or human behaviour to achieve malicious objectives, [3-9].

Malware, a ubiquitous tool in the cyber attacker’s arsenal, encompasses a range of malicious software designed to infiltrate, disrupt, or damage computer systems. This includes viruses, worms, Trojans, ransomware, spyware, and adware, each with its own specific malicious intent, [10]. DoS and DDoS attacks, on the other hand, seek to overwhelm target systems with an excessive volume of requests, rendering them unable to function properly. While DoS attacks originate from a single source, DDoS attacks leverage distributed networks of compromised devices to amplify the assault, [11].

SQL injection exploits vulnerabilities in web applications to execute malicious SQL queries, potentially granting attackers unauthorized access to databases or enabling data manipulation. Similarly, XSS attacks inject malicious scripts into web pages, posing risks such as the theft of sensitive information, [5].

MitM attacks involve intercepting and possibly altering communications between two parties without their knowledge, enabling attackers to eavesdrop or manipulate data. Brute force attacks entail trying numerous combinations of usernames and passwords until the correct one is found, often to gain unauthorized access to accounts or systems, [3].

Social engineering and phishing attacks target human vulnerabilities, manipulating individuals into divulging confidential information or performing actions that compromise security. Phishing, in particular, involves attackers masquerading as trustworthy sources to trick victims into revealing sensitive information or downloading malicious content, [7,8].

Another type of attack is login attack. This malicious activity involves unauthorized entities acquiring login credentials, often through illicit means, to impersonate

legitimate users and gain unauthorized access to crucial systems, [12,13]. In the case of the cyberattack on Latitude, it seems that the method employed falls under the category of a login attack

According to Latitude, the attack came from a major vendor they use. The attacker acquired employee login credentials and used them to steal personal information from backbone service providers. This categorizes the Latitude cyberattack as a login attack, [14].

Type	Description
unpatched software	applications or systems that contain known vulnerabilities that have not yet been addressed through the implementation of updates or patches.
weak passwords	those that are easily guessed by unauthorized users
injection	Flaws allowing untrusted data to be sent to an interpreter as part of a command or query
phishing attacks	A form of online fraud in which hackers attempt to get your private information such as passwords, credit cards, or bank account data.
XSS	Flaws allowing the execution of scripts in the user's browse
zero-day vulnerabilities	a vulnerability in a system or device that has been disclosed but is not yet patched.
misconfigured security settings	occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access
insider threats	when someone close to an organization with authorized access misuses that access to negatively impact the organization's critical information or systems.

Vulnerabilities Exploited in the Latitude Financial System Breach

In the realm of cybersecurity, organizations face a myriad of vulnerabilities that jeopardize their systems and data integrity. Table 1 provides a summary of common vulnerability categories.

In the following, we will analyse every type of vulnerability and investigate their presence within Latitude company. Unpatched software is a critical vulnerability, leaving systems open to exploitation by cybercriminals and the distribution of malware and ransomware. Such breaches can lead to severe consequences, including compromised privacy, damaged reputations, and substantial financial losses, [16].

Weak passwords present another prominent vulnerability, often characterized by their predictable nature, making them susceptible to brute force attacks. Attackers exploit this weakness to gain unauthorized access to sensitive information, compromising system integrity and security. Web applications, crucial for online business operations, are vulnerable to SQL injection attacks due to flaws in their databases. These attacks pose serious threats to data confidentiality and integrity by allowing attackers to execute malicious SQL queries, potentially accessing sensitive information, [17].

Phishing attacks remain a major concern, with attackers employing social engineering tactics to deceive users and

steal credentials. By impersonating trusted entities, attackers exploit user trust to compromise security and gain access to sensitive information, [18].

Cross-site scripting (XSS) attacks enable attackers to execute malicious scripts on victims' web browsers, compromising data and stealing sensitive information. Zero-day vulnerabilities, undisclosed to vendors after release, leave systems vulnerable to exploitation, posing significant security risks.

Misconfigured security settings, such as unchanged defaults or configuration errors, enable unauthorized access, leading to system vulnerabilities.

Lastly, insider threats, whether intentional or unintentional, pose a significant risk, as individuals with authorized access may misuse their privileges to harm the organization. Insider threats encompass both malicious insiders and negligent insiders. Malicious insiders are individuals who intentionally abuse their access privileges to carry out harmful actions against the organization. Negligent insiders are individuals who inadvertently compromise security through careless or uninformed actions. While their intentions may not be malicious, their behaviour can still lead to security breaches, [19].

According to published reports on the Latitude attack case, it appears that SQL injection, phishing attacks, XSS, zero-day vulnerabilities were not utilized for the attack. The primary vulnerability was associated with an insider threat. It remains unclear whether the insider threat was intentional or negligent. Additionally, misconfigured security settings on the backend of a third party likely contributed to the threat not being identified in the initial stage.

Accountability and Motivations in Targeting the Organization

Determining accountability in a cyber-attack is complex, involving examining various factors. At the forefront of accountability are the attackers, whether individual hackers, hacktivist groups, cybercriminal organizations, state-sponsored actors, insiders, or other malicious parties. They bear primary responsibility for cyber-attacks.

Additionally, organizations whose systems were compromised may share some level of accountability. This could stem from inadequate cybersecurity measures, failure to patch known vulnerabilities, poor employee training on security practices, or insufficient incident response protocols.

Third-party service providers also play a role in cyber-attack accountability. If the attack exploited vulnerabilities or weaknesses in systems or services provided by third parties, those providers bear accountability for the breach. This underscores the importance of vetting and monitoring third-party vendors to ensure they adhere to rigorous cybersecurity standards.

Regulatory authorities and government agencies overseeing cybersecurity standards may be accountable if they fail to enforce compliance or offer adequate guidance. Their role in setting and enforcing regulations is crucial. Furthermore, insider employees within an organization pose a significant accountability factor. Whether acting intentionally or unintentionally, insiders can compromise security by leaking sensitive information, circumventing protocols, or falling victim to social engineering tactics. Effective employee training and stringent access controls are essential for mitigating insider threats and minimizing the risk of data breaches.

Determining cyber-attack accountability demands a thorough investigation into root causes, considering legal, technical, and regulatory aspects. In the Latitude cyber-attack case, the majority of accountability appears to lie with an insider employee and a third-party backend provider. The primary accountable party is the insider employee of Latitude who either intentionally or negligently compromised their password. Additionally, the third-party backend provider failed to regularly check for suspicious data access.

The motivations behind such attacks can vary widely, encompassing financial gain, ideological agendas, espionage, and sabotage. In the Latitude case, the motivation was financial. Latitude Financial CEO Bob Belan stated that the hacker demanded a ransom, but the company refused to pay, citing Australian government rules, [20].

Could the incident have been prevented?

Preventing data breaches requires a comprehensive approach involving various policies and procedures. One key aspect is employee training, ensuring that staff are educated on cybersecurity best practices and aware of potential threats. Establishing clear security policies and procedures is essential, outlining guidelines for data handling, access controls, and incident response protocols. Additionally, standard HR policies should be implemented for friendly terminations, including the removal of accounts, passwords, and access privileges on an employee's last work day.

To bolster security measures, it's crucial to recover all keys for encrypted data and physical access, such as door keys and pass cards, ID badges. Removing accounts and passwords prior to notifying an employee of termination can help prevent unauthorized access. Security officers may assist in cleaning out a departing employee's desk or accompany them off premises to ensure compliance with security protocols, [21].

It is unclear to what extent Latitude complies with the mentioned issues. While implementing these policies and procedures can greatly reduce the likelihood of such inci-

dents, achieving zero probability is not guaranteed. Without perfect information on Latitude's comprehensive approach and the inability to eliminate the possibility of such incidents entirely, we cannot definitively say it was avoidable. Another attempt to prevent the leakage of Latitude information after the hack was the consideration of paying a ransom. However, this did not guarantee the prevention of information leaks. Moreover, it violated Australian government regulations regarding ransom payments.

To what extent could Cyber Insurance alleviate the risk?

In the contemporary digital landscape, cyber risk has emerged as a distinct operational hazard for businesses, necessitating proactive measures for mitigation. Cyber insurance serves as a valuable tool in mitigating the aftermath of cyber-attacks by providing coverage for various expenses incurred. This includes the costs associated with investigations, legal fees, business interruptions, and penalties, [22]. The demand for cyber insurance is witnessing a notable surge, driven by the escalating frequency of cyber incidents. Research by Comerford and et al underscores this trend, revealing that over half of all cyberattacks target small- and mid-size businesses. Despite the evident need, a significant proportion of small business owners remain uninsured against cyber risks. This discrepancy can be attributed to several factors. Firstly, many business owners fail to recognize the necessity of cyber insurance, underestimating the potential threats posed by cyber-attacks. Secondly, there is a lack of understanding regarding the scope of coverage provided by cyber insurance policies. Lastly, some business owners erroneously assume that their existing insurance policies adequately safeguard them against cyber-related issues, [22,23].

In light of these findings, it becomes evident that cyber insurance holds substantial promise in mitigating cyber risk. By providing financial protection against the myriad costs associated with cyber incidents, cyber insurance offers a vital safety net for businesses. However, there remains a pressing need for greater awareness and education regarding the importance and scope of cyber insurance coverage. Bridging this knowledge gap is crucial in ensuring that businesses, particularly smaller enterprises, are adequately prepared to confront the evolving cyber threat landscape.

What repercussions have been observed with customers?

In last report Latitude Financial has revealed that 14 million customer records – including driver's licence numbers, passport numbers and financial statements were stolen from its system in mentioned cyber. This report

revealed that the attack was far worse than the company initially reported. The consumer lender, which offers personal loans and credit to customers shopping at stores including JB Hi-Fi, The Good Guys and Harvey Norman said in a statement that some of the document's date back to at least 2005. The details stolen include 7.9 million Australian and New Zealand driver's licence numbers and 53,000 passport numbers, Latitude said. A further 6.1 million customer records were also stolen, of which 5.7 million were provided before 2013. These records include information such as names, addresses, phone numbers and dates of birth, the company said, [24].

Customer's reflection

In this section, we review the reflections and concerns of customers affected by the data breach at Latitude Financial. The breach has had a significant impact on their trust and sense of security regarding their personal information. Many customers have expressed profound distress over the breach of their personal information. The violation of privacy and the potential for identity theft and fraudulent activities due to unauthorized access to sensitive data such as driver's license numbers, passport numbers, and financial statements have left them feeling exposed and vulnerable.

The breach has also raised serious questions about the adequacy of data security measures and regulatory oversight in Australia. Customers have voiced the need for stricter regulations to compel companies to invest more in data security and implement robust policies to ensure data integrity. The retention of information dating back to 2005 by Latitude Financial has particularly concerned customers, calling into question the company's data retention practices and purposes.

Moreover, the response from insurance providers has been deeply disappointing to many customers, exacerbating their frustration and sense of disillusionment. There is a clear consensus that a third party failed to recognize and evaluate the external movement and access effectively, further highlighting the need for better security measures. Additionally, customers have pointed out the possibility of insider involvement, whether intentional or unintentional, which underscores the importance of thorough selection and training processes for employees. They believe that every individual with access to sensitive information should be held accountable for safeguarding it, with measures in place to monitor and mitigate insider threats effectively.

Overall, the data breach at Latitude Financial has highlighted an urgent need for comprehensive reforms in data security practices and regulatory frameworks. Customers whose trust has been shaken by this incident are calling

for meaningful action to prevent similar breaches in the future and to protect the privacy and security of individuals' personal information.

Conclusion

In conclusion, the data breach at Latitude Financial stands as a stark reminder of the pervasive threats posed by cyberattacks and the critical importance of robust data security measures. The breach, which compromised the personal information of millions of customers, has not only undermined trust in the company but has also raised broader concerns about regulatory oversight and the adequacy of data protection practices across industries. The incident underscores the need for stricter regulations to compel companies to invest more in data security and implement comprehensive policies to safeguard sensitive information effectively. It also highlights the imperative of thorough employee selection and training processes to mitigate insider threats and ensure accountability among those entrusted with access to confidential data.

Furthermore, the response from insurance providers in the aftermath of the breach has been disappointing, revealing gaps in coverage and exacerbating customer frustration. This underscores the importance of evaluating and enhancing cyber insurance policies to better address the evolving landscape of cyber risks.

Ultimately, the data breach at Latitude Financial serves as a catalyst for meaningful reforms in data security practices and regulatory frameworks. As customers whose privacy has been compromised, individuals rightfully demand action to prevent similar incidents and uphold the integrity of personal information in an increasingly digitized world. It is imperative for companies and regulatory bodies alike to heed these lessons and prioritize the protection of consumer data as a fundamental aspect of their operations.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: May. 2024 Accepted: Jul. 2024

Published online: Jul. 2024

DOI: 10.22034/ASAS.2024.459650.1058

References

- [1]. Ainsworth K, Terzon E. Millions expected to be affected by Latitude Financial hack, believed to be far worse than initially expected. ABC News [Internet]. 2023 Mar 27; Available from: <https://www.abc.net.au/news/2023-03-27/latitude-far-worse-cyber-hacking-almost-8-million-people/102141364>
- [2]. Barrett J. Latitude Financial cyber-attack worse than first thought with 14m customer records stolen. The Guardian [Internet]. 2023 Mar 27; Available from: <https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen>
- [3]. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 11(4), 89. <https://doi.org/10.3390/fi11040089>
- [4]. Tavakoligolpaygani, S. (2024). Criminal Activity and Environmental Impact as Cryptocurrency Concerns. *Advances in the Standards & Applied Sciences*, 2(1), 1–3. <https://doi.org/10.22034/asas.2023.429605.1048>
- [5]. Aslan, O., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE Access: Practical Innovations, Open Solutions*, 8, 6249–6271. <https://doi.org/10.1109/access.2019.2963724>
- [6]. Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access: Practical Innovations, Open Solutions*, 9, 11895–11910. <https://doi.org/10.1109/access.2021.3051633>
- [7]. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyediji, S., & Porras, J. (2023b). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132, 103387. <https://doi.org/10.1016/j.cose.2023.103387>
- [8]. Prakash, J., Yu, C. C. Q., Thombre, T. R., Bytes, A., Jubur, M., Saxena, N., Blessing, L., Zhou, J., & Quek, T. Q. S. (2021). Countering concurrent Login attacks in “just tap” push-based authentication: A redesign and usability evaluations. 2021 IEEE European Symposium on Security and Privacy (EuroS&P).
- [9]. Chaganti, R., Bhushan, B., & Ravi, V. (2023). A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. *Computer Communications*, 197, 96–112. <https://doi.org/10.1016/j.comcom.2022.10.026>
- [10]. Botacin, M., Ceschin, F., Sun, R., Oliveira, D., & Grégio, A. (2021). Challenges and pitfalls in malware research. *Computers & Security*, 106(102287), 102287. <https://doi.org/10.1016/j.cose.2021.102287>
- [11]. de Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, 222(109553), 109553. <https://doi.org/10.1016/j.com->

net.2022.109553

[12]. Ur Rahman, R., & Tomar, D. S. (2020). Taxonomy of Login attacks in web applications and their security techniques using behavioral biometrics. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 122–139). IGI Global.

[13]. Lala, S. K., Kumar, A., & Subbulakshmi. (2021). Secure Web development using OWASP Guidelines. 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 323–332.

[14]. Latitude Cyber Incident. (n.d.). Com.au. Retrieved April 5, 2024, from <https://www.latitudefinancial.com.au/latitude-cyber-incident>

[15]. Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access: Practical Innovations, Open Solutions*, 7, 168774–168797. <https://doi.org/10.1109/access.2019.2950849>

[16]. Araujo, F., & Taylor, T. (2020). Improving cybersecurity hygiene through JIT patching. *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*.

[17]. Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., & Al-Qassas, R. (2023). A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal A Global Perspective*, 32(4), 252–265. <https://doi.org/10.1080/19393555.2021.1995537>

[18]. Asiri, S., Xiao, Y., Alzahrani, S., Li, S., & Li, T. (2023). A survey of intelligent detection designs of HTML URL phishing attacks. *IEEE Access: Practical Innovations, Open Solutions*, 11, 6421–6443. <https://doi.org/10.1109/access.2023.3237798>

[19]. Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications*, 73(103433), 103433. <https://doi.org/10.1016/j.jisa.2023.103433>

[20]. Cybercrime update 11. (n.d.). Com.au. Retrieved April 5, 2024, from <https://www.latitudefinancial.com.au/about-us/media-releases/cybercrime-update-11-04-2023.html>

[21]. Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, 2023, 115–133. <https://doi.org/10.58496/mjcsc/2023/016>

[22]. Turedi, S., & Erkan-Barlow, A. (2023b). CIO equity compensation and IT investment: the moderating role of board monitoring and evidence of managerial myopia. *Review of Behavioral Finance*, 15(6), 916–934. <https://doi.org/10.1108/rbf-04-2022-0118>

[23]. Yasasin, E., Prester, J., Wagner, G., & Schryen, G. (2020).

Forecasting IT security vulnerabilities – An empirical analysis. *Computers & Security*, 88(101610), 101610. <https://doi.org/10.1016/j.cose.2019.101610>

[24]. Barrett, J. (2023, March 27). Latitude Financial cyber-attack worse than first thought with 14m customer records stolen. *The Guardian*. <https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen>

Submit your manuscript to Advances in the standards and applied sciences journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open Access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

**Submit your next manuscript at:
journal.standards.ac.ir**