GLOBAL DATA BREACH ANALYSIS: SERASA EXPERIAN FEBRUARY 2021

Yemi Adetutu, Patrick Eckland, Jamia Russell, Yinwei Wang, Satvik Yagnamurthy

MSDS 485 - DL_SEC 55

November 10, 2024

A data breach is a security incident in which unauthorized individuals or entities gain access to confidential and sensitive data, typically involving personal, financial, or proprietary corporate information. Data breaches can take many forms, ranging from malicious cyberattacks to human error or system vulnerabilities. When a breach occurs on a large scale, affecting a significant portion of a population or crossing international borders, it is classified as a national or global data breach. These incidents are not only a violation of privacy but can have far-reaching consequences for the individuals affected, as well as the organizations involved. For businesses and institutions, the impacts of a data breach can be devastating, leading to financial losses, reputational harm, legal liabilities, and increased operational costs. The aftermath often requires heightened efforts in cybersecurity, public relations, and regulatory compliance. The frequency and scale of such breaches underscore the pressing need for robust data protection measures, comprehensive regulatory frameworks, and proactive threat detection systems to safeguard sensitive information and minimize the risk of unauthorized access (Ponemon Institute 2021).

In February 2021, one of the largest data breaches in South American history occurred when the personal and financial data of over 223 million Brazilian citizens and 40 million companies were reportedly leaked from Serasa Experian, a major credit bureau in Brazil. The stolen data, which included tax identifiers, full names, addresses, credit scores, and income details, was later found on the Dark Web. It was sold for as little as $0.75 per record, making it easily accessible to cybercriminals and identity thieves. This breach, which exposed vast amounts of highly sensitive information, raised questions about the effectiveness of Serasa Experian's data protection measures. The breach's alignment with Serasa's internal database and the forum's title, "Serasa Experian," led many to believe that the company was involved in the leak, further complicating the situation. Speculation arose that the breach might have been facilitated by internal vulnerabilities, either due to negligence or deliberate malicious action (Belli 2021).

The breach also highlighted concerns about Brazil's data protection laws, specifically the Brazilian General Data Protection Law (LGPD), which had only recently come into effect. While the

LGPD was designed to improve data privacy and security, the Serasa Experian breach demonstrated the challenges in enforcing such regulations effectively, particularly when organizations are ill-prepared to handle and protect large-scale personal data. The breach served as a stark reminder of the complexities involved in safeguarding personal data at a national level, particularly when dealing with large data brokers and the growing sophistication of cyber threats (Daragon 2021).

Impacting more than 223 million Brazilian citizens and 40 million companies, the leak, speculated to have originated from Serasa Experian's database, disclosed sensitive information including unique tax identifiers, dates of birth, first and last names, addresses, education status, salaries, incomes, credit scores and histories, and purchasing power, which was listed on a Dark Web forum (Belli 2021). With this information—available for purchase on the forum for prices ranging from $0.75 to $1—identity thieves were equipped to commit credit theft, tax refund fraud, loan and employment fraud, make fraudulent purchases, and hijack existing accounts. Consequently, organizations were more susceptible to these practices, leading to a heightened need for improved security and verification processes and increased investment in operational costs and customer service to maintain workflow.

Serasa Experian, the alleged source of the leak, suffered significant damage to its public perception due to the accusations against the company. The structure and content of the data, which aligned closely with Serasa's existing databases, and the Dark Web forum's title, "Serasa Experian," led the public to believe the company was involved in the breach (Ventura 2021). In an analysis by Syhunt Icy Team and blogger Felipe Daragon, it was speculated that aspects of the breach "may have been an inside job—carried out deliberately and maliciously by a firm employee" (Daragon 2021). Additionally, Procon, São Paulo's Consumer Rights Foundation, found Serasa Experian's response to the breach insufficient, concurring that the leak most likely originated from within the company and deeming Serasa an untrustworthy organization for business dealings.

At the same time, Serasa Experian was already under investigation for illegal data disclosure and was involved in a lawsuit with the Public Prosecutor's Office of the Federal Territories (MPDFT). The MPDFT alleged that Serasa had engaged in the mass commercialization of client personal data (Ministério Público Federal 2023). The investigation revealed that Serasa was selling consumer data to third parties through customer prospecting services as a way to attract new customers. The Brazilian Federal District Court in Brasília ordered Serasa to cease selling this data or face fines.

Following this major incident, the Secrecy Institute, in conjunction with the MPDFT, filed a civil action proposing that Serasa be held financially liable for the leak. They accused Serasa of not only the illegal selling of personal data but also of "producing a vulnerable environment conducive to fraud" (Ministério Público Federal 2023). Plaintiffs in the civil action argued that Serasa should compensate each affected person with R$30,000 and be ordered to pay a fine equivalent to up to 10% of its annual revenue from the previous year, with a minimum amount set at R$200 million (Ministério Público Federal 2023). The MPDFT and Secrecy Institute also recommended a daily fine of R$20,000 to require Serasa to notify citizens whose data they had sold and exposed on the internet. Lastly, the MPDFT stipulated that within 60 days of conviction, Serasa must implement a more advanced security system with policies to ensure data security and transparency regarding data lineage to mitigate future risks of leakage.

At the time of the Experian data breach, the only legislation in place was the Consumer Protection Code (CDC). Established in 1990, the CDC included provisions for protecting consumer data and privacy and required companies to ensure the security and confidentiality of consumer information. Unfortunately, the CDC was inadequate in preventing the breach from happening, as this broad consumer protection law covered various aspects of customer rights but lacked specificity and detailed requirements for data protection. For example, the CDC did not contain detailed definitions for many key terms, such as "personal data" and "data subjects." Additionally, the CDC did not have a strong enforcement and compliance framework, which meant organizations were not incentivized to implement necessary data

protection measures. Finally, the CDC did not mandate specific technological and procedural measures for data protection, such as encryption, anonymization, and audits.

Ironically, the Brazilian General Data Protection Law (LGPD)—introduced in 2018 but enforced in September 2020—could have largely mitigated the risks, as the Experian breach was mainly caused by unauthorized access to sensitive data. The LGPD includes several provisions targeting such unauthorized access: 1) it requires explicit consent from individuals for data processing; 2) it grants data subjects the rights to access and modify their personal data; 3) it has a notification mechanism that requires companies to notify the national data protection authority in the event of a data breach; and 4) it mandates that companies appoint a data protection officer to ensure compliance with the LGPD. With these provisions in place, there would have been less chance for the data breach to occur on such a large scale. Although the LGPD provides a strong and solid framework, it may still not be fully adequate due to a lack of awareness and training, implementation challenges, and the complexity of data protection. It takes time for companies to fully immerse themselves in LGPD requirements.

Additional guidelines have emerged that could further help mitigate the risks of such an event. By the end of 2022, Brazil's national data protection authority (ANPD) published updated breach guidelines. These guidelines include additional recommendations and an updated breach reporting form that companies must use for regulatory notification. The updated guidelines could have helped with the data breach, as they enhanced the breach notification requirements in terms of both timeliness (e.g., companies must notify ANPD within three business days) and the level of detail (e.g., companies need to include information on affected data subjects, the number of affected subjects, and technical measures adopted). These updated guidelines also focus on high-risk data, such as financial data and personal information, so that protection can be prioritized. Finally, the guidelines indicate a stronger enforcement approach to incentivize companies, like Experian, to implement more robust data protection.

Serasa Experian is responsible for this breach primarily because it happened under their watch. There are a number of other indicators such as past monetization of data and even their response to the media, which was deemed inadequate. The Brazilian government may have also played a role in the data leakage with limited enforcement of The Brazilian General Data Protection Law from 2018-2020. Stricter enforcement for a longer time period before the 2021 leakage would have minimized damages. Just as Equifax was responsible for their 2017 data breach in the United States, prosecutors charged Serasa Experian with the same claims seeking hundreds of millions of dollars in settlement along with 10% of their annual revenue in penalties.

For a strategy to minimize data breach risks, organizations must adopt a holistic approach that includes policies, technology, and oversight. In this breach, there was a loss both on the technical side showing vulnerabilities and on the systemic with governing. A good first start is proper clear data policies. These policies should start with smart access and classification level provisioning that enforces the principle of least privilege, granting employees access only to the data necessary for their roles. This by role-based access control stems, in the event of this breach, this would not impact the company the way it did before. In addition, as a company, it may be recommended to provision limited all level accesses for only certain in campus, internal system based access.

An immediate implementation that will help all companies is the use of multi-factor authentication (MFA) for high-risk systems. As we enter an era where artificial intelligence (AI) is increasingly involved in decision-making and automating human tasks, securing access to sensitive data becomes even more critical. Ensuring robust authentication methods should be a top priority in the discussion, as AI-driven systems handling personal and financial information introduce unique risks. Additionally, the policy should include data classification practices to categorize information based on its sensitivity. This ensures that sensitive data—such as personal details, financial records, and other confidential information—receives stricter protection controls, including encryption and anonymization, to prevent unauthorized access and data breaches.

Monitoring customer trust and satisfaction levels after a breach is critical, as transparency and clear communication can help mitigate reputational damage. By tracking customer behavior, companies can gain valuable insights into emerging risks. With this data, organizations can better understand potential threats and vulnerabilities. Implementing user behavior analytics (UBA) allows companies to detect unusual activities, both internal and external, which could indicate a potential security breach or malicious behavior. Oversight is another crucial element of a robust data protection strategy. Companies should establish clear data ownership policies so that it is known who is responsible for specific data sets or tables. Data owners must oversee compliance with data protection laws and ensure that security protocols are consistently maintained. They should also regularly update employees on data protection best practices to mitigate risks. Effective regulatory compliance requires timely breach notifications to the appropriate authorities, and organizations should conduct regular external audits to assess their data security posture.

Additionally, implementing strong third-party management policies is essential. While internal audits are a key part of data security, they should not be relied upon as the sole measure. Third-party vendors often handle sensitive data or provide critical services, so it's important to conduct thorough due diligence and regular audits to ensure that third parties meet the same security standards as the organization itself. With clearly defined data ownership, organizations can conduct a comprehensive impact analysis to assess the severity of a breach and identify the specific individuals or systems affected. A well-structured data breach prevention strategy should prioritize encryption to protect sensitive data from unauthorized access. Data masking can further minimize risks by ensuring that even if data is exposed, it remains unusable for malicious purposes. To proactively identify potential security threats, organizations should deploy Intrusion Detection and Prevention Systems (IDPS) to monitor network traffic for signs of unauthorized access, alongside automated vulnerability scanning tools to regularly assess and address system weaknesses. In the event of a breach, historical logs can provide valuable insights, helping to identify the users involved and track the source of the issue. This allows organizations

to mediate the situation more effectively. Furthermore, continuous security audits should be conducted to ensure that the organization's policies and practices align with the latest security best practices and regulatory standards. These audits help verify that security measures are effective and up-to-date, ensuring ongoing protection against future breaches.

In conclusion, this comprehensive data breach strategy that integrates robust policies, advanced technology checks, and effective oversight. This is essential for organizations to protect their sensitive data and maintain trust. By continuously adapting to emerging threats and regulatory changes, companies can ensure they remain proactive in safeguarding against data breaches.

References

1. Audi, Amanda. “Prosecutors Go After Credit Monitoring Agency Over Massive Data Leak.” *The Brazilian Report*. Last modified December 6, 2023. https://brazilian.report/liveblog/politics-insider/2023/12/06/prosecutors-go-after-credit-monitoring-agency-over-massive-data-leak/.
2. Belli, Luca. “The Largest Personal Data Leakage in Brazilian History.” openDemocracy. Last modified February 3, 2021. https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/.
3. Business & Human Rights Resource Centre. “Brazil: Largest Personal Data Leakage Exposes 223 Million People and Includes Facial Images, Salary, Credit Score, Addresses, and Tax Identifiers.” Last modified February 3, 2021. https://www.business-humanrights.org/en/latest-news/brazil-largest-personal-data-leakage-exposes-223-million-people-and-includes-facial-images-salary-credit-score-addresses-and-tax-identifier.
4. Chambers and Partners. “6 Months into the LGPD: Lessons and Challenges.” Last modified July 28, 2021. https://chambers.com/articles/6-months-into-the-lgpd-lessons-and-challenges.
5. DLA Piper. “Breach Notification in Brazil.” Last modified January 28, 2024. https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=BR.
6. Experian plc. “Response to Media Speculation in Brazil.” Last modified February 8, 2021. https://www.experianplc.com/newsroom/press-releases/2021/response-to-media-speculation-in-brazil.
7. Mari, Angelica. “Brazilian Government Urged to Protect Consumers from Massive Data Leak.” *ZDNet*. Last modified February 9, 2021. https://www.zdnet.com/article/brazilian-government-urged-to-protect-consumers-from-massive-data-leak/.
8. Mari, Angelica. “Experian Challenged Over Massive Data Leak in Brazil.” *ZDNet*. Last modified February 20, 2021. https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil/.

9. Ponemon Institute. "Cost of a Data Breach Report 2021." Ponemon Institute, 2021. https://www.ponemon.org/research/cost-of-a-data-breach.
10. Pinheiro, Rafael. “Brazil: Data Protection Authority Issues Guidelines on Data Breach Notification.” *Lexology*. Last modified February 15, 2021. https://www.lexology.com/library/detail.aspx?g=f8cba4de-b585-4716-8684-9cb7cdf71024.
11. Procuradoria da República em São Paulo. “MPF Requer da Serasa o Pagamento de Multa Superior a R$ 200 Milhões por Vazamento de Dados Pessoais.” Last modified December 4, 2023. https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/mpf-requer-da-serasa-o-pagamento-de-multa-superior-a-r-200-milhoes-por-vazamento-de-dados-pessoais.
12. The Brazil Business. “Consumer Rights in Brazil.” Last modified January 28, 2024. https://thebrazilbusiness.com/article/consumer-rights-in-brazil.
13. Ventura, Felipe. “Exclusivo: Vazamento Que Expôs 220 Milhões de Brasileiros é Pior do Que Se Pensava.” *Tecnoblog*. Last modified January 25, 2021. https://tecnoblog.net/noticias/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/.

Teamwork

Our team met early in the week to decide on which data breach case to research, and how to assign the assignment criteria. The majority of our team was present for this meeting and the entire team

consistently communicated via text messages throughout the week. This ensured we remained on the same page.

Satvik handled the introduction, Jamia explained consequences, Yinwei discussed legislation, Yemi provided recommendations, and Patrick put together the references while also writing the analysis paragraph and finalizing the teamwork summary. Our team decided on the Serasa Experian story because we wanted to work on an example outside of the United States, which ended up being Brazil. We also preferred researching a credit agency over something in the social media space.