JOISTECH: Journal of Information System and Technology
ISSN 3063-9778 (Media Online)
Vol 01, No 02, Desember 2024, Hal 76-81

Crisis Management and Recovery Strategies After a Data Leak: Equifax Case Study

Ledi Diniyatullah[1*], Kurniati Bunga Rindu[2]

[12]Faculty of Industrial Engineering, Master of Information Systems, Telkom University, Bandung, Indonesia
Email: [1*]ldiniyatullah@student.telkomuniversity.ac.id, [2]kbnrindu@student.telkomuniversity.ac.id

Abstract− The Equifax data breach that occurred in 2017 was one of the largest data security incidents in history, impacting approximately 147 million individuals. This incident highlights the importance of effective crisis management and recovery strategies in the face of cybersecurity threats. This article explains the crisis management and recovery strategies implemented by Equifax following the data breach. This research uses a case study approach to analyze the actions taken by companies in responding to incidents, including crisis communication, security system improvements, and compensation to consumers. In addition, this article also discusses the challenges and failures faced by Equifax, and provides recommendations for future improvements. It is hoped that the findings of this research will provide insight for other companies in developing more effective policies and strategies to deal with data security crises in the future.

Keywords: Crisis Management, Data Privacy, Equifax; Information Security, Post-Data Breach Recovery.

1. INTRODUCTION

Data leaks have become one of the most serious threats in today's digital era, with the potential to damage a company's reputation and threaten the security of users' personal information. Data leaks can be caused by a variety of factors, including sophisticated hacker attacks, human error, or weaknesses in security systems. One prominent example is the data leak that occurred at credit company Equifax in 2017. The incident not only resulted in huge financial losses for the company, but also raised questions about effective crisis management and post-data leak recovery strategies. The Equifax case study offers valuable insight into how a company can respond to and recover from a reputation-damaging data leak.

In March 2017, Equifax Systems was compromised via a vulnerability in the Apache Struts web application. In May-July 2017, unauthorized access was not detected for months, then sensitive data was leaked (Novak & Vilceanu, 2019). In September 2017, Equifax disclosed a data breach, leading to public outcry, a drop in stock prices, and the resignation of its top officials. The cause is a failure in vulnerability management in the web application. Communication breakdowns and a lack of effective IT policies led to it not realizing a vulnerable version of Apache Struts was running on its systems (Petru-Cristian, 2023). The timeline of these events can be seen in the following figure 1.

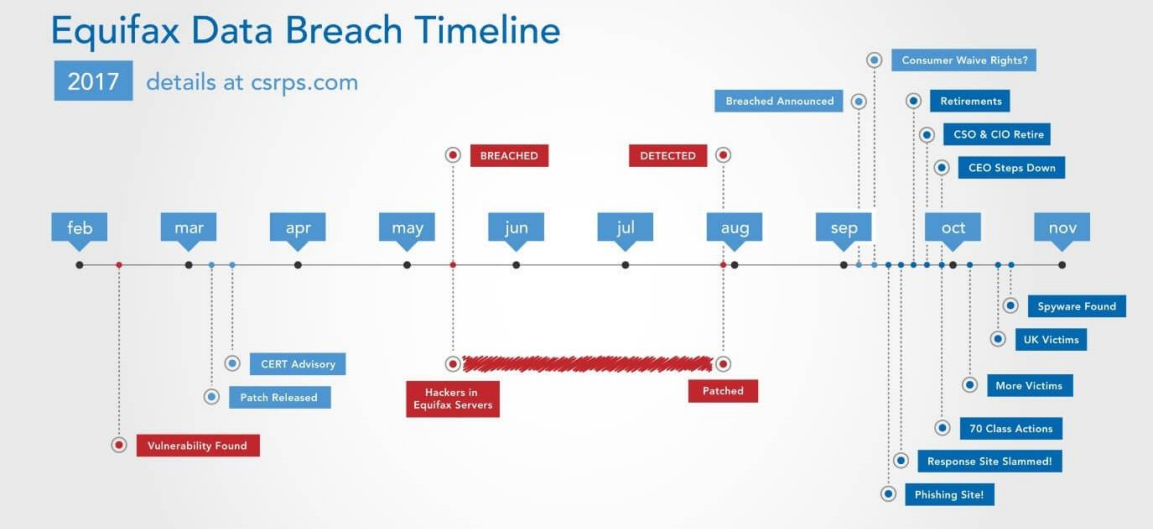

Figure 1. Equifax Data Breach Timeline (Venkatesh Sundar, 2018)

Equifax is one of the world's largest credit reporting agencies, holding the sensitive information of millions of consumers. In September 2017, Equifax announced that it had been the victim of a cyber attack that resulted in the leak of the personal data of 147 million people (Berghel, 2020). The leaked data included names, social numbers, birth dates and other personal financial information. Equifax lacked robust security policies and controls to detect and respond to

intrusions. After the incident, Equifax faced numerous lawsuits, including a class action lawsuit that reached $700 million. This incident highlights the vulnerabilities that exist in large companies' information security systems, as well as the need for effective crisis management strategies.

An effective crisis management strategy in a data leak situation requires quick and coordinated action to mitigate the negative impact. One of the first steps companies must take is to identify the source and scale of the data leak. Equifax must immediately close the security gaps that allowed the attack to occur and stop unauthorized access to their systems. Apart from that, companies also need to carry out a thorough risk evaluation to determine the potential financial and reputational losses that may arise due to data leaks (Kolevski et al., 2021).

After identifying the source of the data leak, the next step is to provide notification to affected consumers and the appropriate supervisory authorities. Equifax must provide clear and accurate information about the type of data that was leaked and the steps it is taking to protect consumers from data misuse. Prompt and transparent notifications can help restore consumer trust and reduce potential reputational damage to companies.

In addition, companies also need to improve the security of their systems and fix existing weaknesses to prevent data leaks in the future. Equifax should conduct regular security audits, improve encryption of sensitive data, and improve security training for their employees. Post-data leak recovery also involves rebuilding a company's reputation through clear and consistent communication with consumers, business partners, and other stakeholders (Bernard Oloo Akello, 2024). Equifax must demonstrate their commitment to improving data security and preventing future data leaks.

In the Equifax case study, an effective crisis management and post-leak recovery strategy required collaboration between various departments within the company, including information security, legal, and corporate communications. Companies also need to learn from their mistakes and continuously improve their information security so as not to repeat the same mistakes in the future. Thus, the Equifax case study provides valuable insight for other companies on how to confront and recover from reputation-damaging data leaks.

2. RESEARCH METHODOLOGY

2.1 Research Stages

The research method used in this research is a descriptive-analytic method with a qualitative approach. Data will be collected through literature studies and document analysis related to the Equifax data leak as well as the response and crisis management strategies implemented by the company. A SWOT analysis was conducted to evaluate the crisis management and post-data leak recovery strategies implemented by Equifax. SWOT analysis is an effective approach to identifying the strengths, weaknesses, opportunities and threats facing an organization in a particular context (Benzaghta et al., 2021). In the context of the Equifax case study, a SWOT analysis will help understand the internal and external factors that influenced the company's response to its data leak .

First, in conducting a SWOT analysis of Equifax's crisis management strategy, the author will evaluate the company's strengths in dealing with data leaks (Hajizadeh, 2019). Equifax is strong in terms of having strong financial resources, a broad network, and extensive experience in the credit industry. These factors can help companies take quick and effective steps to address data leaks and restore customer trust.

Then, the author will look at the weaknesses of Equifax's crisis management strategy. One of the weaknesses that can be identified is the lack of focus on data security before a leak occurs. This can be seen from Equifax's failure to identify and respond to security threats that lead to mass data leaks. Apart from that, slow responses and less effective communication with stakeholders are also weaknesses in their crisis management.

Next, the author will evaluate the opportunities that Equifax can exploit in post-data leak recovery. One opportunity that can be identified is improving data security and transparency in communications with customers to rebuild their trust. Companies can also use this incident as momentum to improve their overall security infrastructure.

Finally, the author will identify the threats faced by Equifax in managing data leaks and post-leak recovery. These threats include the potential loss of customer trust, lawsuits and stricter regulations related to data security, as well as a negative impact on the company's reputation.

By conducting this SWOT analysis , the author was able to identify the key factors that influenced the crisis management and recovery strategy after the Equifax data leak. This analysis can also provide valuable insight for other companies in the same industry facing similar situations in the future.

3. RESULT AND DISCUSSION

This research revealed various important findings regarding the strategies implemented by Equifax following the 2017 data leak. The analysis carried out included identifying strengths and weaknesses in Equifax's response to the incident,

as well as opportunities and threats faced in recovery efforts. By using the SWOT analysis method, this research provides in-depth insight into the effectiveness of the steps taken by Equifax and their implications for public trust and the company's business sustainability.

3.1 IT governance to prevent data leaks

Good IT governance is the main foundation in preventing data leaks that can harm the company. In an ever-evolving and increasingly complex environment, data protection becomes more important as time goes by. Data leaks can be caused by various factors, ranging from hacker attacks to human error (Fowler & Maranga, 2022). Therefore, if a company has strong policies, adequate technology, and a security culture embedded in the organization, it can help reduce the risk of data leaks. By adopting a holistic and proactive approach to data security, companies can reduce the impact of data leaks and maintain their reputation and customer trust.

The following are IT Governance steps that companies can use to prevent data breaches:

a. Carrying out Data Identification and Classification, by identifying sensitive data and classifying it based on its level of importance and sensitivity can help determine the level of security required for each type of data (Li et al., 2023).

b. Create a reliable data security system, by adding a security system consisting of encryption, firewall, VPN and antivirus to protect data from unauthorized access and malware attacks (Aslan et al., 2023).

c. Maintaining password security, by implementing strong access controls and authentication mechanisms, organizations can ensure that only authorized individuals have access to sensitive information. Multi-factor authentication can also be used to prevent unauthorized access. Additionally, using a strong password with a minimum length of 8-16 characters and avoiding common mistakes in creating passwords will help improve security (Suleski et al., 2023).

d. Carrying out routine employee training, routine employee training in IT governance aims to increase employee understanding and skills in managing IT effectively (Osborne & Hammoud, 2017). It includes material on IT governance concepts, control-based risk management, IT governance frameworks and best practices. This training helps employees understand how to manage IT systems, data and services well so that the company can operate more safely and efficiently.

3.2 SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) on Equifax company strategy

A SWOT analysis of Equifax's corporate strategy in dealing with data leaks revealed various strengths, weaknesses, opportunities and threats (Fowler & Maranga, 2022). The SWOT analysis of Equifax's shown in Table 1.

Table 1. The SWOT Table of Equifax's

Strengths	Weaknesses	Opportunities	Threats
Reputation and Experience	Security Incidents	Market Expansion	Adverse Regulatory
Global Reach	Regulatory Dependence	Technological Innovation	Changes
Extensive Data Assets	Intense Competition	Strategic Partnerships	Increasing Competition
Diverse Product Offerings	Cybersecurity Vulnerability	Growing Demand for Data Security	Cybersecurity Threats
Advanced Technology		Services	Economic Fluctuations
		Favorable Regulatory Changes	Litigation and Fines

3.2.1 Strengths

The Strengths of Equifax includes the strong financial capability to invest substantial resources in improving its cybersecurity systems and the capacity to provide free credit monitoring services to affected consumers. Additionally, Equifax has access to leading cybersecurity experts who can help strengthen their security infrastructure.

3.2.2 Weaknesses

The Weaknesses findings included a lack of transparency in initial communications with the public, resulting in confusion and reduced consumer confidence. Additionally, slow responses and complicated compensation procedures add to consumer dissatisfaction.

3.2.3 Opportunities

On the other hand, the opportunities available to Equifax following this incident include the opportunity to repair and strengthen its reputation through significant improvements in data security and operational transparency. Companies can also take advantage of these incidents to develop new, stronger cybersecurity products and services, which can attract consumer trust in the future.

3.2.4 Threats

The Threats faced by Equifax include increased regulatory scrutiny and potential sanctions from regulatory agencies, as well as the risk of litigation from affected consumers. Additionally, loss of consumer confidence can have a negative impact on long-term business, reducing market share and affecting a company's profitability.

This SWOT analysis shows that while Equifax has strengths and opportunities to improve the situation, it must also address significant weaknesses and threats to restore and maintain consumer confidence and business stability.

3.3 The Role of Organizational Culture in Events at Equifax

Organizational culture plays a crucial role in the success or failure of a company, including in the security aspect. Equifax, a company that experienced a major data breach in 2017, shows how organizational culture can impact security (Wijaya, 2019). Here are some cultural factors that can influence security failures:

a. Lack of communication

A culture that cannot encourage effective communication can hinder the exchange of information about security risks. If employees don't feel free to report problems or ask questions, potential security gaps may be overlooked.

b. Micromanagement

If management unduly limits employee creativity and initiative, this can hamper the organization's ability to identify and address security threats.

c. Lack of clear expectations

A culture that does not set clear expectations regarding security can lead to a lack of clarity in the actions that must be taken to protect data and systems.

d. Fast hiring and firing

If an organization does not evaluate candidates well before hiring them, unsuitable new staff can destroy the culture and result in high employee turnover.

In optimizing security, companies need to build a culture that encourages open communication, transparency and risk awareness (Salahdine & Kaabouch, 2019). Additionally, ensuring that security values are embedded throughout the organization is an important step to avoid security failures like those that occurred with Equifax.

3.4 Strategies that can be implemented to prevent data breaches

The Equifax, a major credit institution, has experienced significant data security incidents in the past, highlighting the importance of effective security risk management. To overcome these challenges, Equifax needs to adopt new strategies that are more proactive in managing data security risks, increasing security awareness, innovating in security technology, and complying with relevant data security regulations, Equifax can reduce future security risks and rebuild trust with customers and other stakeholders (Bima Pamungkas, 2021).

Here are some recommended strategies that can help Equifax mitigate future risks:

a. Improved IT Security

Companies need to adopt the latest security technologies, such as data encryption, use of VPN (Virtual Private Network), and regular software updates. For example, Target Corporation experienced a data breach in 2013 due to a weakness in their security system, resulting in millions of customer data being stolen (Bima Pamungkas, 2021).

b. Employee Education and Training

Companies must provide training on cybersecurity to employees so they understand threats and how to address security risks. For example, Uber's data breach in 2016 occurred due to a phishing attack that managed to compromise user data due to a lack of security awareness (Syafira, 2020).

c. Access Rights Management

Companies must ensure that access rights to sensitive data are limited according to job requirements. For example, the Equifax data breach in 2017 occurred due to a security flaw that allowed hackers to access sensitive customer credit data (Hapsari & Pambayun, 2023).

d. System Activity Monitoring

Companies must monitor system activity continuously to detect suspicious activity or potential attacks. For example, the Yahoo data breach in 2014-2016 occurred due to an attack that went undetected for months (Rosati et al., 2019).

e. Implementation of Strict Security Policies

Companies must have clear and strict security policies, and ensure that they are adhered to by all employees and business partners. For example, the Sony data breach in 2011 occurred due to security flaws caused by weak security policies (Aswandi et al., 2020).

By implementing these strategies, companies can reduce the risk of data breaches and protect sensitive company information and customer data.

4. CONCLUSION

In dealing with data security crises such as data leaks, good IT governance is the key to preventing similar incidents from occurring in the future. Equifax experienced challenges in their IT governance, especially in strengthening security systems and managing appropriate access rights. A SWOT analysis of Equifax's corporate strategy revealed some strengths, such as strong financial resources, but also identified weaknesses in its crisis response, such as a lack of transparency in communications. To prevent data breaches, strategies that can be implemented include improving IT security, employee education and training, strict management of access rights, monitoring system activity, and implementing strict security policies. Companies can learn from Equifax's mistakes and successes in dealing with this data security crisis, and take proactive steps to strengthen their security systems and respond quickly if future incidents occur. Thus, companies can reduce the risk of data breaches and protect their sensitive information as well as customer data.

REFERENCES

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics (Switzerland)* (Vol. 12, Issue 6). MDPI. https://doi.org/10.3390/electronics12061333

Aswandi, R., Rofifah, P., Muchsin, N., & Sultan, M. (2020). *PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS)*. https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebar-

Benzaghta, M. A., Elwalda, A., Mousa, M., Erkan, I., & Rahman, M. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights*, *6*(1), 55–73. https://doi.org/10.5038/2640-6489.6.1.1148

Berghel, H. (2020). The Equifax Hack Revisited and Repurposed. In *Computer* (Vol. 53, Issue 5, pp. 85–90). IEEE Computer Society. https://doi.org/10.1109/MC.2020.2979525

Bernard Oloo Akello. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 148–162. https://doi.org/10.30574/wjaets.2024.11.1.0152

Bima Pamungkas, R. (2021). *LEMAHNYA PERATURAN HUKUM PERLINDUNGAN DATA PRIBADI: STUDI KASUS EQUIFAX DI AMERIKA SERIKAT PADA 2017*.

Fowler, B., & Maranga, K. (2022). *CYBERSECURITY PUBLIC POLICY SWOT ANALYSIS CONDUCTED ON 43 COUNTRIES* (1st ed.). CRC Press.

Hajizadeh, Y. (2019). Machine learning in oil and gas; a SWOT analysis approach. *Journal of Petroleum Science and Engineering*, *176*, 661–663. https://doi.org/https://doi.org/10.1016/j.petrol.2019.01.113

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021). Cloud computing data breaches: A review of U.S. regulation and data breach notification literature. *2021 IEEE International Symposium on Technology and Society (ISTAS)*, 1–7. https://doi.org/10.1109/ISTAS52410.2021.9629173

Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-01757-0

Novak, A. N., & Vilceanu, M. O. (2019). "The internet is not pleased": twitter and the 2017 Equifax data breach. *Communication Review*, *22*(3), 196–221. https://doi.org/10.1080/10714421.2019.1651595

Osborne, S., & Hammoud, M. S. (2017). Effective Employee Engagement in the Workplace. *International Journal of Applied Management and Technology*, *16*(1). https://doi.org/10.5590/ijamt.2017.16.1.04

Petru-Cristian, N. (2023). *A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications*. https://doi.org/10.13140/RG.2.2.17461.65763

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. *International Journal of Accounting*. https://doi.org/10.1142/S1094406019500136

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). MDPI AG. https://doi.org/10.3390/FI11040089

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. In *Digital Health* (Vol. 9). SAGE Publications Inc. https://doi.org/10.1177/20552076231177144

Syafira, A. (2020). *UPAYA SEKURITISASI PEMERINTAH INGGRIS DALAM KEBIJAKAN KEJAHATAN CYBER WANNACRY TAHUN 2017*.

Venkatesh Sundar. (2018, February 2). *Lessons from Poor Vulnerability Protection by Silicon Valley Companies*. Indusface. https://www.indusface.com/blog/poor-vulnerability-protection-silicon-valley-companies/

Wijaya, M. (2019). PERAN BUDAYA ORGANISASI DALAM MENGOPTIMALKAN EFEKTIFITAS DAN EFISIENSI STRATEGI ORGANISASI. *Media Informatika*, *18*(2), 67–74.