STEP EARLY AND TREAT: SOLUTIONS FOR REDUCING DATA BREACHES WITH CORPORATE SOCIAL RESPONSIBILITY AS TWO COMPLEXING LAYERS OF PROTECTION

Arif Budi Raharja [1*], Ngurah Made Novianha Pynatih [2] , Zaenal Aripin [3]

[1] STIE YKP,Yogyakarta, 55184, Indonesia, budiraharja1970@gmail.com

[2] Universitas Tabanan, Tabanan, 82121, Indonesia, pynatih3@gmail.com

[3] Universitas Sangga Buana, Bandung, 40124, Indonesia, Zaenal.arifin@usbypkp.ac.id

Abstract

The increased use of information technology has brought great benefits to modern organizations, but has also increased the risk of data breaches. In facing these challenges, the Go Early and Cure approach has been proposed as a complementary strategy to reduce the risk of data breaches. The Go First approach emphasizes prevention before a data breach occurs, while the Treat approach focuses on rapid response after a data breach occurs. Corporate Social Responsibility (CSR) also plays an important role in supporting both approaches by raising awareness, strengthening data protection and improving relationships with external stakeholders. However, implementing both approaches faces a number of challenges, including a corporate culture that may not support data security practices, limited resource availability, and varying data security awareness among organizational members. To overcome these challenges, organizations need to prioritize building a culture that supports data security, allocate resources efficiently, and continuously increase awareness of cyber security risks. By addressing these challenges, organizations can strengthen their layers of protection against data breaches and maintain stakeholder trust.

Keywords: Data Breach, Stepping Early, Remedy, Corporate Social Responsibility, Data Security.

Introduction

As we enter an increasingly advanced digital era, the problem of data breaches is becoming more complex and frequent. Organizations, both large and small, are increasingly vulnerable to cyber security threats that can result in sensitive data leaks and major financial losses. In facing these challenges, an effective data protection strategy is critical. Two approaches that are gaining increasing attention in the business community are Going Early and Cure, and Corporate Social Responsibility. Both have a crucial role to play in reducing the risk of data breaches and providing better protection for companies and their consumers.

Stepping Early is a proactive approach that emphasizes preventing data breaches in the first place. This includes steps such as implementing strict security policies, training employees on cybersecurity practices, and using advanced security technologies such as data encryption and continuous network monitoring. One of the main advantages of this approach is its ability to prevent data breaches

before they occur, saving a company time, money, and reputation. By making the right investments in infrastructure and human resources, organizations can significantly reduce risks and build a strong foundation for the security of their data.

On the other hand, the Treat approach focuses on responding quickly and effectively to data breaches after they occur. This involves rapid identification of threats and vulnerabilities, recovery of lost or affected data, and transparent communication with stakeholders such as customers, business partners, and regulatory authorities. The key to this approach is the ability to act quickly and mitigate the negative impact of a data breach. While it does not replace the need for preventive measures, Treatment is an important additional layer of protection in keeping data secure.

Corporate Social Responsibility (CSR) is a principle that is increasingly recognized in the modern business world. This includes a company's commitment to acting ethically and contributing to the well-being of society, the environment and the economy as a whole. In the context of data protection, CSR can be manifested in a variety of ways, including investment in innovative security technologies, participation in industry initiatives to improve data security standards, and supporting education and awareness efforts about cyber security in society. By adopting a strong CSR approach, companies can strengthen their reputation as responsible leaders and build better relationships with consumers and other stakeholders.

When Stepping Early and Treating is combined with the principles of Corporate Social Responsibility, they form two complementary layers of protection in mitigating the risk of data breaches. Through this approach, companies can build a solid foundation for the security of their data, while fulfilling their moral and ethical obligations to society. In doing so, they not only protect themselves from potential financial and reputational losses caused by data breaches, but also play an active role in building a safer and more trustworthy digital ecosystem for all parties involved.

Method

In the qualitative research on "Going Early and Cure: Solutions to Mitigate Data Breaches with Corporate Social Responsibility as Two Complementary Layers of Protection", a literature study method will be used to investigate relevant literature on data security, responsible business practices social, and data protection approaches that have been adopted by leading companies. The research population consists of business organizations in various sectors and sizes that have an interest in strengthening the security of their data and maintaining corporate reputation. The research sample will be selected purposively, including companies that are considered leaders in implementing the "Go Early" and "Treat" strategies and have a strong commitment to Corporate Social Responsibility.

Data collection techniques will involve in-depth interviews with organizational leaders, information security managers, and CSR practitioners to gain a deep understanding of the strategy, challenges, and impact of the approach. In addition, document analysis and case studies will also be used to collect relevant secondary data to support research findings. With this combination of methods, this research is expected to provide in-depth insight into the effectiveness and benefits of combining Stepping Early, Cure, and Corporate Social Responsibility as two complementary layers of protection in reducing the risk of data breaches.

Results and Discussion

Stepping Early and Treating are two complementary approaches to reducing the risk of data breaches in organizations. The Go First approach emphasizes prevention before a data breach occurs, while the Treat approach focuses on responding quickly and effectively after a data breach occurs. Corporate Social Responsibility (CSR) also plays an important role in supporting both approaches, by raising awareness, strengthening data protection and improving relationships with external stakeholders. However, there are a number of challenges that need to be overcome in implementing both approaches, including a corporate culture that may not support data security practices, limited resource availability, and varying data security awareness among organizational members.

Main Challenges	Influence on Going Early	Effect on Treating
Company Culture	It may hinder the implementation of strict security policies and active participation of the entire organization in protecting sensitive information.	Resistance to change or inability to recognize the importance of data security as a strategic priority.
Resource Availability	May discourage investment in advanced security technology and providing adequate training for staff.	Limits an organization's ability to adopt new security solutions or provide intensive training for staff.
Awareness of Data Security	Low awareness can increase the risk of unsafe behavior or negligence caused by a lack of knowledge.	A lack of awareness can hinder rapid response to data breach incidents and prevent timely recognition of signs of an attack.

Company culture, resource availability, and awareness of data security have a significant impact on the implementation of Step Early and Cure as

complementary layers of protection. A company culture that supports data security and active participation from across the organization can facilitate the implementation of strict security policies and ensure a rapid response to data breaches. However, challenges related to organizational culture can arise when there is resistance to change or a lack of recognition of the importance of data security as a strategic priority. Additionally, the availability of adequate resources, both in terms of financial and human resources, is important for implementing advanced security technologies and providing adequate training for staff.

However, organizations with limited budgets or limited human resources may have difficulty meeting these challenges. Furthermore, awareness of data security is also an important factor in ensuring the success of both approaches. A lack of awareness of cyber security risks can increase the risk of a data breach because staff may not recognize the signs of an attack or take unsafe actions that could open the door to attackers. Therefore, organizations need to continuously increase awareness of data security through ongoing training and awareness campaigns. By effectively addressing these challenges, organizations can strengthen their layers of protection against data breaches and minimize the risks associated with information security.

Implementing a Move Early and Treat approach can effectively reduce the risk of data breaches across organizations

Implementing the Go Early and Treat approach is crucial in efforts to reduce the risk of data breaches in various organizations. The Step Early approach, which emphasizes prevention before a data breach occurs, includes several key factors that contribute to the effectiveness of this strategy. One of them is the strict security policy implemented by the organization. This policy should cover all aspects of data security, from the use of strong passwords to restricted access policies. Implementing clear and comprehensive security policies will help prevent unauthorized access to sensitive data and reduce the risk of data breaches. Additionally, employee training is also an important factor in the Go Early approach. Employees need to be trained on cyber security practices, such as how to recognize phishing attacks or secure their devices while traveling. By increasing employee awareness and skills in dealing with security threats, organizations can reduce the risk of incidents caused by human error or unsafe behavior.

Not only that, security technology also plays a crucial role in the Go First approach. Organizations need to adopt advanced technologies such as firewalls, data encryption, and intrusion detection systems to protect their IT infrastructure from cyber attacks. This system not only helps prevent unauthorized access, but also provides the ability to detect and respond quickly to emerging threats. Additionally, continuous network monitoring is also necessary to identify suspicious activity and take appropriate action before it is too late. By combining

strong security policies, employee training, and advanced security technology, implementing a Step First approach can significantly reduce the risk of data breaches across organizations.

Meanwhile, the Treat approach focuses on responding quickly and effectively to data breaches after they occur. It also involves several important factors that can help reduce the impact of a data breach. One key factor is an organization's ability to identify and respond to data breaches quickly. This includes the use of advanced intrusion detection systems and security analytics to monitor network activity and identify potential threat indicators. Additionally, having a structured and tested incident response plan is key to effectively coordinating an organization's response when a data breach occurs. This plan should include steps such as isolation and recovery of affected data, communication with stakeholders, and post-incident evaluation to correct existing weaknesses.

Corporate Social Responsibility (CSR) can also play an important role in the Medicine approach. Organizations need to recognize the impact that data breaches may have on customers, business partners and society as a whole. As part of their social responsibility, companies must be prepared to take responsibility for data breach incidents and provide appropriate compensation to the affected parties. This not only helps repair the damage caused by the incident, but also builds trust and a strong reputation among stakeholders. Additionally, organizations can also use data breach incidents as an opportunity to improve their security practices and contribute to industry-wide data protection efforts.

However, while both approaches have the potential to reduce the risk of data breaches, there are still several challenges that need to be overcome. One of them is the cost and complexity of implementation. Implementing strict security policies and advanced security technologies can require significant financial investments and require skilled technical resources. In addition, organizational awareness and acceptance of the need for strong data security can also be an obstacle, especially in organizations that do not prioritize aspects of their IT security. Therefore, to successfully reduce the risk of data breaches, organizations need to address these challenges with a holistic approach that includes aspects of policy, training, technology and organizational culture.

Overall, implementing a Move First and Treat approach can help reduce the risk of data breaches across organizations by considering factors such as security policies, employee training, and implemented security technologies. By combining proactive prevention with rapid and effective response to incidents, organizations can build a strong layer of protection to protect their sensitive data and maintain customer trust. However, to successfully implement this approach, organizations need to overcome challenges such as cost, complexity, and an organizational culture that prioritizes data security. Thus, through strong

commitment and a holistic approach, organizations can achieve their goals of reducing the risk of data breaches and maintaining the integrity of their data.

The role of Corporate Social Responsibility in supporting the Go Early and Treat strategy in reducing data breaches

Corporate Social Responsibility (CSR) plays an important role in supporting the Go Early and Cure strategy in reducing data breaches. As part of their commitment to sustainability and societal well-being, companies must recognize that data protection is not only an internal matter, but also their external responsibility towards their stakeholders. One of CSR's main roles is to raise awareness of the importance of data security among external stakeholders, including customers, business partners and the wider community. This can be achieved through education and information campaigns about cyber security threats, best practices for protecting personal data, and steps taken by companies to safeguard sensitive information. By increasing understanding and awareness of data security among the public, CSR can help create an environment that is more aware of the risks of data breaches and encourage acceptance of the steps taken by companies to protect their data.

In addition, CSR's contribution to strengthening data protection also involves investing in innovative security technologies and efforts to improve industry standards regarding data security. Companies can use their CSR funds to develop or adopt new security solutions that can help prevent, detect and respond to data breaches more effectively. This could include developing more sophisticated security systems, using artificial intelligence to analyze potential threats, or investing in research and development to create new, safer technologies. Additionally, companies can participate in industry initiatives or partnerships to improve overall data security standards. This may include collaborating with competitors, governments, and non-profit organizations to develop guidelines and best practices that can be adopted by the entire industry.

Furthermore, the role of CSR in strengthening data protection is also related to improving company relationships with external stakeholders, such as customers and business partners. When companies demonstrate their commitment to data security and their responsibility towards the protection of sensitive information, this can strengthen stakeholder trust and loyalty to the company brand. This is important because trust and reputation are invaluable assets in today's competitive business environment. By strengthening relationships with customers and business partners through socially responsible business practices, companies can reduce the risk of losing business or reputation due to a data breach. In addition, improving relationships with external stakeholders can also help companies overcome the social and legal consequences of data breaches that occur. By building strong partnerships with stakeholders, companies can work together to overcome challenges and strengthen data protection collectively.

However, while CSR contributions can help strengthen data protection and a company's relationships with external stakeholders, there are several challenges that need to be addressed. One is the gap between rhetoric and action, where companies may demonstrate their commitment to CSR but fail to implement practices consistent with those values. To overcome these challenges, companies need to ensure that their social responsibility is integrated into all aspects of their operations, including data security. Additionally, limited resources and financial pressures can be barriers to implementing CSR initiatives aimed at strengthening data protection. Therefore, companies need to allocate sufficient resources to prioritize data security as part of their social responsibility.

Overall, Corporate Social Responsibility has an important role in supporting the Go Early and Cure strategy in reducing data breaches. Through investments in education, technology, and industry partnerships, CSR can help raise awareness, strengthen data protection, and improve a company's relationships with external stakeholders. However, to succeed, companies need to overcome challenges such as gaps between rhetoric and action, as well as limited resources. With a strong commitment and holistic approach, companies can leverage the role of CSR to protect their sensitive data and strengthen their reputation as socially responsible leaders.

The main challenges organizations face in implementing a Go Early and Treat approach

There are a number of key challenges organizations face in implementing a Go Early and Treat approach as complementary layers of protection in mitigating data breaches. One of the main challenges is a company culture that may not support proactive data security practices. In some organizations, awareness of the importance of data security may be low, and information security is considered the responsibility of only the IT department without active participation from the entire staff. A culture that does not support data security can hinder the implementation of a Go First approach, because without the support and participation of the entire organization, the security policies implemented may be ineffective. Additionally, challenges related to organizational culture can also arise when there is resistance to change or an inability to recognize the importance of data security as a strategic priority. Therefore, to successfully implement a Go First approach, organizations need to build a culture that prioritizes data security and ensures that all members of the organization are actively involved in protecting sensitive information.

Furthermore, resource availability is another challenge often faced by organizations in implementing a Go Early and Cure approach. Implementing strict security policies and advanced security technologies requires significant financial investment, as well as skilled human resources to manage and maintain the system. Organizations with limited budgets or limited human resources may face

difficulties in adopting advanced security solutions or providing adequate training for their staff. In addition, resource availability challenges may also relate to the time and effort required to implement the organizational changes required to support the Going Early approach. For example, a company may need to change internal policies, provide intensive training, or integrate new security systems with existing infrastructure. Therefore, in facing the challenge of resource availability, organizations need to carry out careful planning and efficient resource allocation to ensure successful implementation of the Go First approach.

In addition, awareness of data security is also an important factor influencing the successful implementation of the Move Early and Treat approach. This level of awareness can vary among members of an organization, depending on the individual's background, training, and experience. A lack of awareness of cyber security threats and best practices for addressing them can increase the risk of data breaches because staff may not recognize the signs of an attack or take unsafe actions that could open the door to attackers. Therefore, the Step Up First approach requires efforts to increase data security awareness across the organization through regular training, awareness campaigns, and education about cyber security risks. On the other hand, data security awareness is also important in the Treat approach, as a fast and effective response to a data breach requires that all members of the organization recognize the importance of quick action in the face of a security incident. Therefore, organizations need to continue strengthening data security awareness and provide ongoing training to their staff to reduce the risk of data breaches and improve incident response.

In the context of implementing these two approaches as complementary layers of protection, factors such as corporate culture, resource availability, and awareness of data security have a significant impact on the success of the strategy. A company culture that supports data security will facilitate the implementation of strict security policies and ensure active participation from all members of the organization in protecting sensitive information. Meanwhile, the availability of adequate resources will enable organizations to adopt advanced security technologies and provide adequate training to their staff. On the other hand, a high level of data security awareness will help prevent data breaches by reducing the risk of unsafe behavior or negligence caused by a lack of knowledge. Therefore, organizations need to address these challenges with a holistic approach that includes the development of a supportive culture, efficient resource allocation, and ongoing training to ensure successful implementation of these two approaches as complementary layers of protection.

Conclusion

In conclusion, implementing a Go First and Cure approach in reducing data breaches in organizations requires a deep understanding of the challenges faced, including company culture, resource availability, and data security

awareness. A company culture that supports data security, the availability of adequate resources, and a high level of awareness among staff are key to the success of both approaches. Therefore, organizations need to prioritize building a culture that strengthens data security, allocates resources efficiently, and continuously raises awareness of cyber security risks. By addressing these challenges, organizations can strengthen their layers of protection against data breaches and protect their sensitive information, thereby strengthening their reputation as socially responsible leaders and maintaining stakeholder trust.

Bibliography

Aripin, Z., Fitrianti, NG, & Fatmasari, RR (2023). Digital Innovation and Knowledge Management: The Latest Approaches in International Business. A Systematic Literature Review in the Indonesian Context. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 62-74.

Aripin, Z., Mulyani, SR, & Haryaman, A. (2023). MARKETING STRATEGY IN PROJECT SUSTAINABILITY MANAGEMENT EFFORTS IN EXTRACTIVE INDUSTRIES: BUILDING A RECIPROCITY FRAMEWORK FOR COMMUNITY ENGAGEMENT. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 25-38.

Aripin, Z., Haryaman, A., & Sikki, N. (2024). INCENTIVE STRUCTURE AND ITS EFFECT ON REFERRALS: AN ANALYSIS OF THE ROLE OF SELF-CONSTRUCTION AS A DETERMINANT. *KRIEZ ACADEMY: Journal of development and community service* , *1* (2), 65-77.

Hanuun, NNP, Negara, MRP, & Aripin, Z. (2023, December). ENTREPRENEURIAL EMPOWERMENT IN CREATING SUSTAINABLE DEVELOPMENT IN DEVELOPING COUNTRIES: TO WHAT EXTENT DO THEY STRENGTHEN AND CONTRIBUTE TO EACH OTHER?. In *Journal of West Java Economic Society Networking Forum* (Vol. 1, No. 1, pp. 54-63).

Aripin, Z., Sikki, N., & Fatmasari, RR (2024, January). AN IN-DEPTH EXPLORATION OF EMPIRICAL RESEARCH ON ENTREPRENEURIAL MINDFULNESS: A SYSTEMATIC LITERATURE REVIEW TO EXPLORE NUANCES, FINDINGS, AND CHALLENGES. In *Journal of West Java Economic Society Networking Forum* (Vol. 1, No. 2, pp. 1-15).

Negara, MRP, & Aripin, Z. (2023, December). Manage Insurance Customer Satisfaction with Premiums and Perceived Quality Assessments. In *Journal of West Java Economic Society Networking Forum* (Vol. 1, No. 1, pp. 21-37).

Wibowo, L.A., & Ariyanti, M. (2023, December). UTILIZATION OF ARTIFICIAL INTELLIGENCE SYSTEMS TO PREDICT CONSUMER BEHAVIOR. In *Journal of West Java Economic Society Networking Forum* (Vol. 1, No. 1, pp. 45-53).

Mardhika, R., de Fretes, CHJ, & Simanjuntak, TR (2023). Indonesia's Interests in Indonesia–France Defense Cooperation Relations: (Case Study: Purchase of Dassault Rafale Fighter Aircraft in 2020–2022). *Multidisciplinary Scientific Journal* , *2* (04), 43-55.

Nareswari Rasendriya, L., Marisa Kurnianingsih, SH, & MH, MK (2024). *Fulfilling the Rights of Victims of Sexual Violence (Comparative Study of Indonesia and Malaysia)* (Doctoral dissertation, Muhammadiyah University of Surakarta).

Raharjo, B. (2021). Fintech Financial Technology Digital Banking. *Prima Agus Teknik Foundation Publishers* , 1-299.

Wibowo, A. (2023). Legal and Technology Dispute Resolution. *Prima Agus Teknik Foundation Publishers* , 1-168.

Tanjung, R., Mawati, AT, Ferinia, R., Nugraha, NA, Simarmata, HMP, Sudarmanto, E., ... & Silalahi, M. (2021). Organization and management.

Wahyuni, S. (2023). PUBLIC SERVICE MANAGEMENT: Optimizing the Protection of Victims of Violence against Women and Children.

Wibowo, A. (2021). Change Management (Change Management). *Prima Agus Teknik Foundation Publishers* , 1-180.

Zen Munawar, ST, Kom, S., Kom, M., Putri, NI, Kharisma, IL, Kom, M., ... & MM, M. (2023). *Information Systems Security: Basic Principles, Theory, and Engineering Application of Concepts* . Kaizen Media Publishing.

M ARIFKI, ZAINARO (2023). EXEMPLARY LEADERSHIP, SOCIAL VALUE, AND CULTURAL VALUE TO BUILD TRUST TO IMPROVE PRECEPTOR PERFORMANCE.

Bernadetha, SKM, Nurhidayati, SK, Nasrullah, N., Basri, HM, ST, S., Bugis, DA, ... & Pemayun, IDGA (2023). *Introduction to health promotion and health behavior* . MEDIA PATNERS STRAIT.

Fajri, LRHA (2023). THE ROLE OF MOBILE ADHOC IN DATA COMMUNICATION. *Prima Agus Teknik Foundation Publishers* , 1-209.

Bustami, MR, Mudzakkir, M., & Nasruddin, E. (2021). *CSR ISLAM Seven Principles of Organizational Transformation for the Progress of Business and Society* (Vol. 1). UMMPress.