Cross-Border Data Security: Analysis of High-Profile Violations and Mitigation Strategies

Riska Nofharina Lutfiah*
Department of Government Affairs and Administration, Jusuf Kalla School of Government, Faculty of Social and Political Sciences, University Muhammadiyah Yogyakarta, Yogyakarta, 55183, Indonesia
riskalutfiah62@gmail.com

Tunjung Sulaksono
Department of Government Affairs and Administration, Jusuf Kalla School of Government, Faculty of Social and Political Sciences, University Muhammadiyah Yogyakarta, Yogyakarta, 55183, Indonesia
tunjungsulaksono@umy.ac.id

Abstract

This study investigates patterns of large-scale data breaches at Facebook (2019), SolarWinds (2020), Tokopedia (2020), and LinkedIn (2021) using a qualitative descriptive case study method. Data were obtained from credible media sources, academic articles, and official publications and analyzed using the CIA Triad paradigm (Confidentiality, Integrity, Availability). Results show that confidentiality is the most frequently violated dimension, mainly due to weak Application Programming Interface (API) controls and inadequate encryption. Integrity and availability also emerge as major issues in supply chain cases. The analysis follows technical, administrative, and physical controls outlined in ISO/IEC 27002 and NIST SP 800-Rev. 1. This study highlights the importance of integrating technical safeguards with global regulatory frameworks, including the European General Data Protection Regulation, China's Personal Information Protection Law, and Indonesia's Personal Data Protection Law. Theoretically, it validates the CIA Triad as a risk classification tool and proposes mitigation strategies to strengthen cybersecurity resilience across jurisdictions.

Keywords: Cross-border data security, data breaches, CIA Triad, encryption, API protection, cybersecurity policy

Introduction

The surge in cross-border data transfer has led to increased data breaches spanning multiple jurisdictions. This trend is exacerbated by the lack of standardized international regulations and the uneven levels of data protection among various locations (Feys et al., 2023; Liu et al., 2024). State and non-state entities are increasingly executing data breaches for objectives such as espionage, economic harm, and propaganda dissemination. Prominent examples include the SolarWinds breach, which targeted the cybersecurity of the US government and companies. Other significant occurrences encompass violations of governmental websites and extensive cyber intrusions, such as the Unique Identification Authority of India (UIDAI) breach (Mone et al., 2024; Yang et al., 2022). In 2015, a significant data breach transpired, notable for its magnitude and extent: the Office of Personnel Management (OPM) infiltration. A group of Chinese hackers executed the theft of 21.5 million federal employee background records and 5.6 million fingerprints (Gootman, 2016). The growing dependence

* Corresponding Author

on digital data, cloud computing, and mobile devices has broadened the attack surface for hackers. Organizations frequently have difficulties in safeguarding data at rest, in use, and in transit, resulting in increased breaches (Ameen et al., 2021; Botha et al., 2017).

Privacy leaks have emerged as a critical security concern that complicates the administration and authentication of personal information, thus hampering communication efficiency between various entities (Guo et al., 2018). As a virtual entity, Facebook has surpassed the combined population of the three countries with the largest populations: China, India, and the United States (Lee, 2021). It has repeatedly faced public scrutiny due to significant data privacy scandals. In 2018, the Cambridge Analytica case revealed how personal data from approximately 87 million users was harvested without consent through a third-party quiz app and later used to influence political campaigns (Isaak & Hanna, 2018). A year later, in 2019, another serious breach occurred when malicious actors scraped data from 533 million users across 106 countries by exploiting Facebook's contact importer feature. Although Facebook fixed the vulnerability in August 2019, the leaked data, which included phone numbers, full names, Facebook IDs, emails, and other profile information, was only publicly circulated on hacker forums by April 2021 (Sun, 2023). Several official sources, including Meta, acknowledged this incident, confirming that scraping practices had extracted data from its platform prior to September 2019 (Clark, 2021). Despite the massive scope of exposure, empirical findings show that news of Facebook data breaches during 2016-2019 did not consistently significantly affect the company's share value (Hinds et al., 2020). In light of the extensive exposure, Facebook opted not to inform the impacted users, eliciting criticism from regulators and privacy activists about its management of the breach and its deficiency in openness.

In addition to reputational damage, as illustrated by the Facebook scandal, the increases in data breaches also impose significant financial burdens, underscoring the economic pressure organizations face and eroding user trust (Ayyagari, 2020; Bansal, 2018). Long-term consumer impact can hinder business operations, cause revenue loss, and worsen a company's reputation (Rahman & Nemati, 2024; Shahul Ikram, 2024). In a cross-border context, data breaches exacerbate cyber risks such as ransomware and advanced persistent threats (APTs) involving sophisticated and difficult-to-detect attack methods (Hamid & Huda, 2025; Teoh & Mahmood, 2017). Although cyber threats are becoming increasingly complex, the effectiveness of technology management and implementation remains a determining factor in mitigating their impact (Li et al., 2023).

Following various data breaches, one of the most systemic attacks with widespread impact occurred in the SolarWinds incident, which, according to Oladimeji & Kerner (2023), was one of the most significant cybersecurity incidents in 2020. It not only impacted a single company but triggered a comprehensive supply chain attack that compromised over 18,000 clients, including multiple levels of the US government. SolarWinds, a major software company, inadvertently distributed a malicious update to its Orion IT monitoring platform, enabling attackers to covertly implant malware onto users' systems. This incident significantly compromised the integrity and confidentiality of thousands of networks and organizations (Lazarovitz, 2021; Sterle & Bhunia, 2021). Bulgurcu & Mashatan (2024) underscore that this breach revealed fundamental deficiencies in incident response coordination and third-party risk management across several industries. The New York State Department of Financial Services (DFS) also noted that the attack revealed the failure of many institutions to classify Orion as a critical vendor despite its broad system access (New York State Department of Financial Services, 2015). Meanwhile, the Cybersecurity and Infrastructure Security Agency (Cybersecurity and Infrastructure Security Agency, 2021) and the United States Government Accountability Office (US Government Accountability Office, 2022) have recognized this occurrence as a critical moment for implementing Zero Trust Architecture and the enhancement of national-level supply chain resilience.

Given the scale and complexity of breaches like SolarWinds, governments worldwide have responded by enforcing more rigorous legislation to enhance openness and accountability in data management. One of the most comprehensive frameworks is the European Union's General Data Protection Regulation (GDPR), which mandates breach disclosure within 72 hours under Article 33 and imposes significant penalties for noncompliance (Zhuo et al., 2021). This regulation has increased breach reporting and pressured organizations to improve data management processes (Mackie et al., 2017;

Malatras et al., 2017; Yan, 2024). However, the effectiveness of such regulations varies across jurisdictions.

The Cambridge Analytica Facebook scandal in 2018 clearly illustrates the weakness of regulations in protecting personal data in the digital age. An estimated 87 million user profiles were exploited to manipulate political campaigns without informed consent (Foecking et al., 2021). The Federal Trade Commission (FTC) imposed a record fine on Facebook and mandated sweeping privacy reforms (Bendix & Mackay, 2022; Federal Trade Commission, 2019). Similarly, the UK's Information Commissioner's Office (ICO) published a detailed investigation into unlawful data use in political advertising (Carroll, 2021; Information Commissioner's Office, 2019). The New York Department of Financial Services (NYDFS) highlighted Facebook's insufficient transparency and weak user data protections in its 2021 report (New York State Department of Financial Services, 2015). The Ministry of Communication and Informatics (Kominfo), Republic of Indonesia, responded to Facebook's hack by requesting clarification and promoting national data privacy legislation (Agustini, 2021). These examples highlight global concern over data privacy and uneven enforcement practices across nations.

Reflecting this global trend, Indonesia, in the Southeast Asian context, has introduced its comprehensive framework, the Personal Data Protection (PDP) Law (Law No. 27/2022) (Government of Indonesia, 2022), which marks a national commitment to align with global standards on privacy and data security. Following the 2020 breach affecting 91 million user accounts, Kominfo compelled Tokopedia to conduct internal audits and notify affected users (Riskinaswara, 2020). The compromised data allegedly contained user ID, email, name, date of birth, gender, and encrypted password (CNBC, 2020). Indrawati & Putri (2021) observed that this violation marked a pivotal moment in trust management within Indonesia's digital marketplace.

One large-scale data breach that exposed Application Programming Interface (API) security weaknesses occurred on the LinkedIn platform, where unknown actors extracted and sold more than 700 million user profiles on the dark web, compromising personal information such as geolocation, salary, email, and phone numbers (Share, 2021; CNN Indonesia, 2021). Although LinkedIn officially denied the occurrence of a breach and claimed it had only used public data (LinkedIn Corporate Communications, 2021), cybersecurity experts argue that this poses a serious privacy risk due to unauthorized data scraping (Nicko, 2021). Gibson et al. (2021) categorized the incident as an API-level vulnerability and emphasized the need for stronger authentication and anti-bot mechanisms.

These incidents underscore a broader issue: the digital ecosystem is rapidly evolving, bringing forth complex security challenges impacting diverse sectors and stakeholders. Cybercriminals use more complicated techniques, like Advanced Persistent Threats (APTs), designed to be undetected for extended periods while stealing important information (Bhardwaj, 2024; Preethi et al., 2024). Integrating AI-powered defense systems has become crucial to modern cybersecurity frameworks (Rangrez et al., 2024). Nonetheless, the advancement of intelligent technologies has also introduced new forms of vulnerabilities, particularly in the convergence of cyber and AI-related threats (Fauzi & Sembiring, 2023). Emerging technologies like quantum computing pose risks to existing encryption mechanisms, while blockchain offers novel methods for securing digital transactions (Radanliev, 2024).

To deal with these complicated threats, strong cybersecurity measures and flexible strategies are necessary to keep digital assets safe and private, as shown by different real-life events (Sharma & Zamfiroiu, 2023). The core components of cybersecurity include encryption and access control (Firmansyah, 2024). Advanced Encryption Standard (AES) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) are two widely adopted encryption standards for securing communications between devices and servers (Arunkumar & Kousalya, 2018; Goluboff, 2015). Cloud computing environments commonly use a load balancer to manage high traffic volumes (Ajagbe et al., 2022). In addition, Amazon Web Services (AWS) offers API-driven infrastructure that enhances agility, automates the infrastructure management lifecycle, and allows flexible experimentation with scalable architectures (Campbell, 2020).

One major challenge in global cybersecurity lies in regulatory fragmentation, as different countries have different data protection regulations. For example, the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), China's Personal Information

Protection Law (PIPL), Japan's Personal Information Protection Act (APPI), and South Korea's Personal Information Protection Act (PIPA) serve as examples of data protection legislation (Lim & Oh, 2025). New EU members from Central and Eastern Europe (CEE) typically exhibit greater efficiency in transposing EU regulations than their Western counterparts (Zhelyazkova et al., 2017). The GDPR, in contrast to the norms of the United States and Canada, operates under distinct jurisdictions; nonetheless, all frameworks consider situational risks and threats to individual data subjects and promote encryption (Heimes, 2016). Divergences in national data regulatory frameworks present issues for other nations, exacerbating the fragmentation of the global regulatory landscape, fostering uncertainty, and escalating compliance costs for enterprises (Shelepov, 2022). The European Union supplements the GDPR with data protection agreements involving non-EU nations, and considers the EU-US Privacy Shield agreement as having the most significant practical effect (Veit, 2022; Yan, 2024).

The different ways countries handle data protection show much inconsistency in global rules, especially when countries rely solely on ISO-based standards. This practice can result in gaps in complying with GDPR regulations. Such a situation requires the integration of information governance (IG) and enterprise architecture management (EAM) to bridge these gaps (Zaguir et al., 2024). In business-to-government data sharing, an accountability gap frequently exists. Corporate digital responsibility (CDR) can function as a conduit between accountability frameworks grounded in public law and those based on data protection law (Schneider, 2022). Enforcing data protection requirements such as GDPR necessitates substantial organizational and technical modifications, posing challenges for firms, particularly within the IT sector (Poritskiy et al., 2019). Companies must cultivate a data protection culture instead of prioritizing swift compliance to avoid penalties. This cultural transformation may result in more sustainable and efficient execution of data protection procedures (Lugati & de Almeida, 2022).

On the other hand, several global data protection frameworks, such as the GDPR and China's PIPL, aim to mitigate cross-border risks by enforcing encryption, breach notification, and data transfer assessment. Article 32 of the GDPR mandates security measures to ensure confidentiality and integrity, which has led to improved compliance among EU-based organizations (Zhuo et al., 2021). The evaluation suggests that GDPR enforcement has improved compliance practices among EU-based companies (Buckley et al., 2022). The Tokopedia breach exemplifies a failure to uphold such standards, with 91 million records exposed due to insufficient encryption. Likewise, the Facebook Cambridge Analytica case reveals access control and data governance weaknesses. Although Indonesia's Personal Data Protection Law (PDP Law; Law No. 27/2022) lacks extraterritorial reach, it incorporates global best practices such as breach notification and accountability. These efforts reflect a broader move to harmonize cybersecurity policies and establish enforceable norms across jurisdictions.

Various cybersecurity policy and system design fields have successfully implemented the CIA Triad approach. In cloud-based systems, the CIA concept helps create honeypots to detect attacks, demonstrating its effectiveness in monitoring threats (Subhash et al., 2024). These findings are consistent with incidents at Tokopedia and LinkedIn, where cloud configuration errors threatened data confidentiality and availability. In the public sector, Kenya and the United States have adopted CIA principles in their electoral systems through biometric and blockchain technologies (Irungu & Girma, 2023). A similar approach should also be applied in other large systems. For example, the data breach incident at Facebook (2019) and the supply chain attack on SolarWinds (2020). Another study used the CIA Triad to evaluate 45 UAV communication scenarios, but the results vary significantly depending on the context and methodology (Shoufan & Damiani, 2017). The study showed that while the CIA Triad is flexible, its application still requires a systematic and standardized approach.

On the other hand, most previous research has focused on technological solutions such as artificial intelligence, blockchain, and identity management (Khare & Raghuwanshi, 2024; Rangrez et al., 2024; Souabni et al., 2022) without directly linking them to the effectiveness of cross-border data protection regulations. Few studies have explored how integrating technology strategies and regulatory frameworks can mitigate cross-border data security risks (Ameen et al., 2021; Xu et al., 2025). Many organizations adopt standards such as ISO/IEC 27001 or NIST SP 800-53 for Information security management practices (Zaguir et al., 2024). However, various studies highlight the challenges of

implementing these frameworks, including resource limitations, dependence on organizational culture, and high administrative burdens—especially for MSMEs (Longras et al., 2018; Mera-Amores & Roa, 2024). Meanwhile, the CIA Triad is also influenced by organizational context (Shojaie et al., 2016). However, it offers a more straightforward and flexible classification framework for mitigation strategies across jurisdictions (Rahman & Nemati, 2024).

Regarding regulation, the European Union, China, and Indonesia have adopted policies such as the GDPR, PIPL, and the Personal Data Protection Law to strengthen cross-border data privacy protection. However, the effectiveness of these policies in mitigating global data security risks has rarely been analyzed in an integrated manner (Lim & Oh, 2025). Existing studies remain sectoral and do not systematically link technical vulnerabilities with mitigation policies.

Most data breach studies—such as the LinkedIn, Facebook, and SolarWinds cases—have also not used standardized evaluation frameworks (Bulgurcu & Mashatan, 2024; Foecking et al., 2021; Gibson et al., 2021). For example, the Tokopedia study emphasizes reputation responses and national policies without direct links to structured mitigation strategies (Indrawati & Putri, 2021; Wibowo et al., 2024). Thus far, only a limited number of studies have systematically applied frameworks such as the CIA Triad to classify vulnerabilities and evaluate the effectiveness of data protection policies across different jurisdictions.

Therefore, this study proposes using the CIA Triad as an integrated evaluation framework to assess the effectiveness of cross-jurisdictional data protection policies. This research seeks to fill a gap in the literature that has not yet systematically examined the relationship between vulnerability classification and cross-border data mitigation policies. This study covers (1) applying the CIA Triad framework to case studies of real-world significant data breaches, (2) evaluating the effectiveness of global data protection regulations in mitigating security risks, and (3) developing mitigation strategies that integrate technological and political approaches. This study seeks to contribute to a more cohesive, actionable, and globally relevant approach to cross-border data protection, offering practical insight for policymakers and cybersecurity professionals alike.

Literature Review

Concept of Data Protection Crossing Borders

In the digital era, data transmission is an essential element of globalization and worldwide collaboration. Nonetheless, data privacy and security difficulties persist, with limited solutions available for safeguarding personal data during cross-border transmission due to the complexities of managing sensitive information across many countries and regions (Liu et al., 2024; Peng et al., 2023). Cross-border data flows encompass international economic concerns and pose challenges to personal information protection, national data security, and the jurisdiction of legal and law enforcement authorities (Liu, 2022). Safeguarding personal information constitutes a significant contemporary regulatory challenge (Yan, 2024). In the realm of globalization, transnational data flow presents numerous problems to international investment law (Wang, 2024). At present, there exists no globally recognized standard for data protection (Alekseenko, 2022).

The CIA Triad model, a prevalent architecture in cybersecurity, comprises three essential components: confidentiality, integrity, and availability (de Oliveira Albuquerque et al., 2014). This methodology offers a systematic framework for enterprises to evaluate and alleviate cybersecurity hazards. Confidentiality safeguards sensitive data from unauthorized access, a significant issue exemplified by incidents including Facebook (2019), Tokopedia (2020), and LinkedIn (2021), during which malicious actors compromised user data. Integrity ensures that data remains unmodified and reliable, pertinent to events such as the SolarWinds (2020) breach, where assailants compromised software supply chains. Availability guarantees that information systems are functional and accessible when required, a vital consideration for enterprises dependent on cloud and internet services (Bulgurcu & Mashatan, 2024; Gibson et al., 2021; Indrawati & Putri, 2021; Sun, 2023). Among the major incidents compromising confidentiality, the 2019 Facebook scraping case stands out due to its vast international scope, affecting over 500 million users across multiple jurisdictions. Although the 2018 Cambridge Analytica case

remains the most widely cited in academic discourse, the 2019 incident presents a distinct example of large-scale data exposure via API vulnerabilities, making it particularly relevant within the CIA Triad framework.

In contemporary global competitiveness and collaboration, digital trade regulations focused on transnational movement have emerged as a competitive advantage for a country (Chin & Zhao, 2022). A practical legal framework for cross-border data transfer is crucial to balancing national security, commercial interests, and individual privacy (Tan, 2024). Since digital trade often includes personal data agreements from the World Trade Organization (WTO) and bilateral and regional trade agreements, it is important to understand how policies limiting the free movement of information between countries affect this table (Marengo, 2020).

Trends and Patterns of Data Violation

Data breaches have been on the rise since 2005, with a marked increase in the number and impact of breaches yearly (Fleury-Charles et al., 2022; Holtfreter & Harrington, 2015; Stottler, 2024). For example, from 2010 to 2018, there were 2,529 violations affecting 194.74 million individual records (Hossain & Hong, 2019). Data breaches in the public sector are also significant, with contextual government factors impacting the incidence and level of violations (Hamid & Huda, 2025; Joseph, 2018). Investors react negatively to data breaches, perceiving them as indicators of internal deficiencies within affected companies (Juma'h & Alnsour, 2021). Mega breaches, involving the loss of a million records or more, have been a significant concern. These large-scale breaches often result from compromised internal structures and systems (Fritz & Kaefer, 2017; Hossain & Hong, 2019).

The impact of data breaches can vary significantly depending on the type of information stolen, with sensitive personally identifiable information (SPII) breaches leading to higher costs and more class-action lawsuits (Poyraz et al., 2020). The CIA Triad framework facilitates the analysis of breaches by assessing the compromise of confidentiality, integrity, and availability in significant data occurrences. For instance, attackers frequently exploited insufficient access restrictions (confidentiality), introduced harmful code (integrity), or disrupted services (availability), underscoring persistent vulnerabilities in cybersecurity systems.

Regulations and Data Security Standards

The introduction of regulations like GDPR has imposed severe penalties for data breaches, pushing organizations to adopt better data protection measures (Tachepun & Thammaboosadee, 2020). Understanding the factors contributing to breaches, such as human error and internal vulnerabilities, is crucial for developing effective cybersecurity strategies (Portalatin et al., 2021). The General Data Protection Regulation has elevated privacy to a status commensurate with security in data protection (Treacy et al., 2020). To mitigate data protection problems, global authorities and standards organizations have issued numerous pieces of legislation, guidelines, and software controls applicable to cloud data (Joshi et al., 2020). Complete frameworks delineating technical, administrative, and legal standards are essential for safeguarding important systems and sensitive information (Volchkova, 2019).

Security includes assessing at-risk data, evaluating data vulnerabilities, and analyzing strategies to mitigate threats to an acceptable risk level (Mary, 1999). The emphasis is on the secure management of data to guarantee the privacy of client information and the protection of company data (Bajaj, 2012). The General Data Protection Regulation (GDPR) will be implemented in the European Union (EU) in May 2018 to address contemporary difficulties concerning personal data protection and to standardize data protection throughout the EU (Tikkinen-Piri et al., 2018). Regulation has escalated expenses and internal administrative procedures. Little case law results in ambiguity (Buckley et al., 2022).

Trust-Minimization Models in Cyber Risk Prevention

Zero trust (ZT) is a way of thinking and planning that helps cybersecurity teams create secure areas and improve data safety by carefully using new technologies, managing risks, and understanding threats

(Wang et al., 2022). The organization lacks data on the quantitative assessments of ZTA's pros and cons (Adahman et al., 2022). Zero trust posits that all trust points must undergo scrutiny and mitigation, security measures will protect individual resources, and the network will not serve as the primary basis for trust. This approach restricts threat mobility and mitigates harm (Simpson, 2022). Access is granted based on the minimum permissions required for a user to perform their job, reducing the risk of unauthorized access (Seaman, 2023).

The financial repercussions of data breaches are substantial for organizations and society. Organizations can gain advantages by comprehending the fundamental elements that affect the probability and consequences of a data breach (Bobbert & Timmermans, 2023). Companies and government entities consistently implement Zero Trust security to validate cybersecurity protocols (Kroculick, 2024). However, organizations frequently encounter difficulties evaluating their advancement in Zero Trust Architecture (ZTA) implementation (Ilyas et al., 2024). Adopting Zero Trust Architecture must consider scalability, user experience, and operational complexity (Verma et al., 2024). The findings indicate that adopting Zero Trust Architecture (ZTA) leads to an average decrease of $684,000 in risk impact over four years for small- to medium-sized enterprises and large organizations (Adahman et al., 2022). Although Zero Trust Security Architecture has become the dominant approach to replacing traditional perimeter-based network security models, this approach is not entirely free from weaknesses. The control center and authentication database in the Zero Trust architecture create new vulnerabilities that are susceptible to centralized attacks. Additional security systems are necessary to strengthen ZT (Guo et al., 2022).

In addition to Zero Trust, threat modeling techniques such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) from Microsoft are esteemed techniques employed to detect security vulnerabilities in software systems. In an empirical study, 57 computer science students assessed the costs and efficacy of STRIDE (Scandariato et al., 2015). It has been applied in various domains, including healthcare, smart homes, and automotive infotainment systems, demonstrating its versatility and effectiveness in different contexts (Ben-Nakhi et al., 2023; Das et al., 2024; Hossain & Hasan, 2023; Viswanathan & Prabhu, 2021). Both models contribute to a trust minimization paradigm that supports proactive threat mitigation, especially in cross-border and multijurisdictional systems.

Empirical Study on ISO/IEC 27001 Standards, NIST Framework, and GDPR Compliance

Information security and privacy compliance have recently become increasingly complex due to escalating regulatory constraints, evolving legislation, and heightened public awareness (Anwar & Gill, 2020). Bringing together the ISO 27001:2013 and ISO 9001:2015 standards into a company's Information Security Management System (ISMS) and Quality Management System (QMS) makes it even more important to safeguard Information and Communication Technologies (ICT) (Hasibovic & Tanovic, 2024). ISO/IEC 27001 is an international standard that provides a structural framework for establishing, implementing, and maintaining an information security management system (ISMS), offering comprehensive guidelines for auditors and implementers. Its application supports governmental or corporate organizations in systematically managing information security risks and ensuring the continuous protection of data assets (Putra et al., 2021). Recognized globally, ISO/IEC 27001 is one of the most widely adopted and authoritative benchmarks in information security (Malatji, 2023).

Adherence to the General Data Protection Regulation (GDPR) or analogous legislation by enterprises may necessitate organizational and technological modifications (Zaguir et al., 2024). Following the implementation of the General Data Protection Regulation (GDPR) in the EU, organizations must modify their business operations and implement suitable technical and organizational safeguards to safeguard the personal data they handle (Diamantopoulou et al., 2020). There is alignment between the security controls in ISO/IEC 27001:2013 and the data protection requirements set out in the GDPR. Therefore, it is necessary to implement security control measures based on ISO/IEC 27001 to fulfill data protection obligations under GDPR provisions. Further identification and mapping of organizations implementing ISO/IEC 27001 is important to ensure their readiness to comply with GDPR (Diamantopoulou et al., 2020).

Cybersecurity Governance Challenges in the Global South

Developing nations frequently lack robust national cybersecurity frameworks. African countries confront distinct issues, notably the swift expansion of internet access coupled with a deficiency in cybersecurity skills, rendering them more susceptible to cybercriminal activities (Von Solms, 2019). Jamaica's establishment of a National Cybersecurity Framework (JNCF) underscores the necessity of integrating international standards and best practices to safeguard national information (Dennis et al., 2014). South Africa's critical role within the BRICS bloc underscores the necessity for synchronized cybersecurity initiatives to capitalize on the advantages of international collaboration (Mitrovic & Thakur, 2019). Cybersecurity training and education are essential for enhancing digital trust and confidence. South African students reported substantial alterations in their online protective habits throughout the epidemic, highlighting the significance of cybersecurity knowledge (Tick et al., 2021).

Developing nations encounter distinct issues regarding cybersecurity (Jacobs et al., 2016). Standard cybersecurity maturity models from wealthy nations often do not meet the unique needs of developing countries because of differences in their development, politics, society, and economic environments (Lee et al., 2025). Least Developed Countries (LDCs) necessitate cybersecurity plans that tackle their specific issues, such as restricted technical progress and insufficient policy frameworks. An integrated approach utilizing modern technology, extensive policy measures, and capacity-building activities can improve national cybersecurity (Hamidi & Singh, 2024). Studies comparing the cybersecurity postures of countries like Pakistan and Indonesia highlight the need to enhance legal frameworks, invest in technical infrastructure, and increase regional and international cooperation (Sadat et al., 2025).

The Role of Artificial Intelligence in Cyberthreat Detection and Prediction

The ability to find and reduce cybersecurity risks, like network breaches, attacks from bad actors, and unknown vulnerabilities, has dramatically improved with AI, especially through machine learning and deep learning (Dhanushkodi & Thejas, 2024). Artificial intelligence (AI) and machine learning (ML) techniques represent the latest developments in computing, including approaches inspired by biological systems such as deep neural networks, which mimic the way the human brain's neural networks work (Nijim et al., 2022). In the context of defense, AI contributes significantly to enhancing protection strategies, system resilience, adaptability, and efficiency through responses to environmental dynamics (Kumar & Ranganathan, 2023).

The use of large language models (LLMs) in cybersecurity offers both opportunities and risks, necessitating mitigation strategies to ensure their development and implementation are conducted securely (Kucharavy et al., 2024). In cloud computing environments, important aspects of data security include node authentication, mutual authentication, the use of digital certificates, and the implementation of strict access controls (Jonnala et al., 2023).

Some examples of AI applications in cybersecurity include cyber threat intelligence (CTI), an innovative AI-based methodology for collecting, analyzing, and handling ongoing and potential attacks that could harm an organization's digital assets (Alguliyev et al., 2023). Additionally, quantum cryptography offers a promising defense against threats from quantum computing, providing high-level encryption based on the principles of quantum physics (Sharma et al., 2024).

Another method is a routing system that relies on trust and uses machine learning to find harmful nodes during Distributed Denial of Service (DDoS) attacks and data packet issues, which improves network security (Ahmed et al., 2023). However, we must design robust and understandable AI models to ensure system trust and reliability. Significant challenges remain, including large-scale data management and real-time processing requirements (Dhanushkodi & Thejas, 2024). So, creating hybrid models, making real-time explanations possible, and using standard ways to measure and ethical guidelines are important for improving AI-based cybersecurity in the future (Mohale & Obagbuwa, 2025).

Technology Approach to Data Security Mitigation

As part of the mitigation approach, technologies such as artificial intelligence (AI)-based anomaly detection have become complementary elements in modern cyber defense frameworks. Risk

management in information technology (IT) can no longer be viewed solely as a technical task but as a crucial managerial function in ensuring the security and sustainability of organizational processes (Alshahrani et al., 2022). A layered security framework is essential in environments such as the Industrial Internet of Things (IoT). This approach includes preventive measures such as anomaly and intrusion detection systems and responsive measures such as incident response plans and data backup strategies (Vetrivel et al., 2024). Proactive cybersecurity strategies, like checking for risks, setting up strict rules, using multi-factor authentication, and regularly updating systems, are important for lowering weaknesses (Berki et al., 2018). Additionally, ongoing training programs and users' comprehension of security tools play a critical role in improving compliance behavior and fostering digital resilience (Adams & Liu, 2021).

The integration of AI-based cybersecurity solutions, such as machine learning-powered anomaly detection, has gained significant attention recently. However, the adoption of such technologies also introduces new risks, including the potential for adversarial attacks and ethical challenges in their implementation (Abbo & Tchomte, 2024). Therefore, ensuring the integrity and confidentiality of data across various platforms remains a critical priority (Pigola & de Souza Meirelles, 2024). Compliance with international standards and regulatory frameworks is essential to maintaining the long-term effectiveness of information security systems (Mizrak & Reyhan Akkartal, 2024). Prevention remains the most effective approach to addressing cyber threats, as history has shown that no regulation has yet succeeded in eliminating data security breaches globally.

Methodology

This research adopts a qualitative case study methodology to examine data vulnerabilities in four major incidents: Facebook (2019), SolarWinds (2020), Tokopedia (2020), and LinkedIn (2021). These cases were selected based on their prominence, cross-sectoral nature, and representation of core vulnerabilities across the CIA Triad dimensions. Data were collected from academic literature, official publications, regulatory documents, and credible news media. Cross-validation between sources is performed to ensure data reliability and consistency.

Figure 1 shows the CIA Triad framework (Confidentiality, Integrity, Availability) was used to identify the main weakness in each incident and help create a plan to reduce risks according to international standards. Along with the CIA Triad as the main framework, this study also includes important parts of the ISO/IEC 27001 and NIST SP 800 series to understand the technical, administrative, and physical controls that were present or missing in each case. These standards were not applied as standalone evaluation models but were used to identify common best practices and implementation gaps, as reflected in the comparative matrix of analyzed incidents.

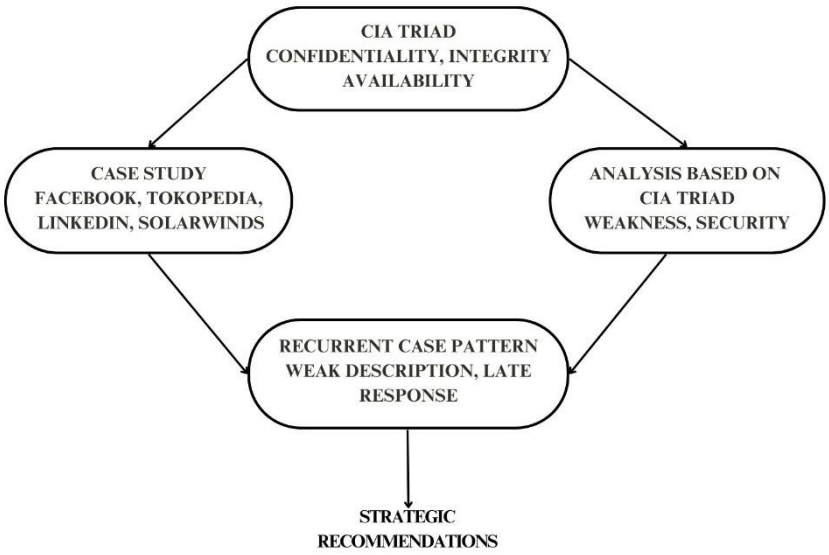

Figure 1. Conceptual Framework of the Study

Results

The following section illustrates the complexity and common patterns of cross-border data breaches. This study analyzes four large-scale data breaches that occurred between 2019 and 2021. The four cases—Facebook, LinkedIn, Tokopedia, and SolarWinds—were selected because they represent technical vulnerabilities and caused significant impacts on millions of users across various jurisdictions. Each case is analyzed based on the security vulnerabilities exploited, the impact caused, and the organization's response following the incident.

1. Facebook's (2019) weakness: scraping that exploited public system features, especially the contact importer. The impact: 533 million user data exposed, including personal information such as name, ID, and location or address. Organizational response: Facebook did not admit any system violations but did fix the server settings.
2. SolarWinds (2020), weakness: Malware inserted in software updates, exploiting the supply chain. The impact: 18,000 organizations affected, including government agencies. Organizational response: changing their software development procedures
3. Tokopedia (2020), weakness: Insufficient encryption for Tokopedia user data leaves 91 million users susceptible to data leakage. The impact: The leakage of personal information puts Tokopedia account users' privacy at risk. The organization responded by confirming that payment data was secure.
4. LinkedIn (2021), weakness: The poorly protected API allows data scraping by unauthorized parties who want to misuse LinkedIn user data. The result was the theft and sale of 700 million user records on the dark web. The organization responded by stating that there was no direct hack.

Figure 2 shows a visualization of the general patterns of weaknesses, impacts, and responses in the four data breaches that were analyzed. This diagram is designed to show the interrelationships between elements and reinforce the identification of recurring patterns. This visualization forms the basis for developing relevant and cross-case mitigation recommendations. It also emphasizes the need for a systematic and standardized mitigation approach.

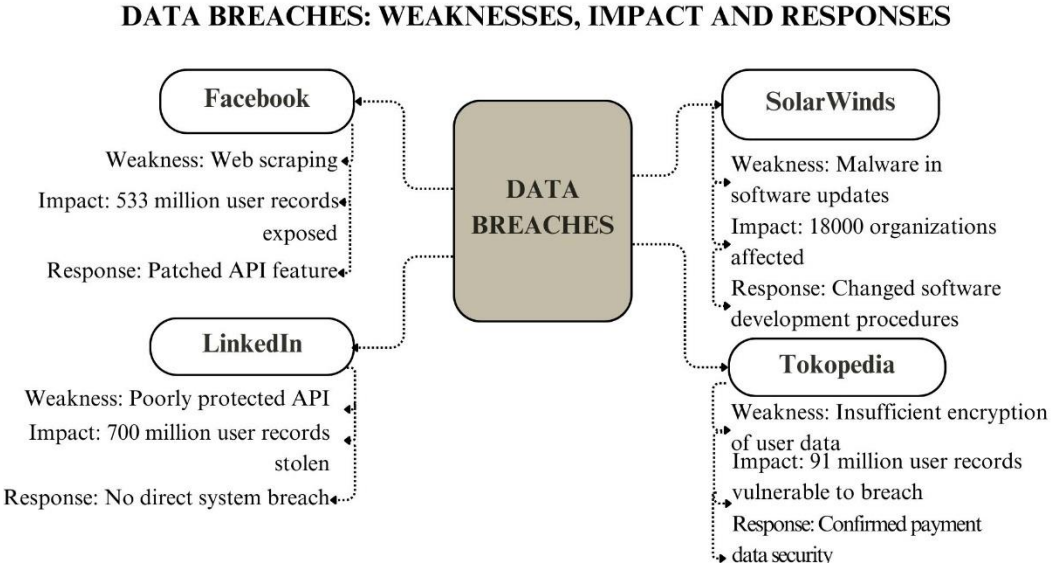

Figure 2. Case Analysis of Data Breach Incidents

Figure 3 illustrates the exploitation of system vulnerabilities and corresponding organizational responses across the four analyzed cases. The analysis identifies three recurring technical weaknesses: (1) insufficient encryption of user data, (2) poor API protection allowing mass data scraping, and (3) supply chain compromise via malware injection in software updates.

Figure 3. Cybersecurity Breach Response Flow Chart

These vulnerabilities were exploited through distinct mechanisms. In the Facebook case (2019), the weakness was the absence of access restrictions on the contact importer API, which enables massive scraping of public metadata. In the Tokopedia case (2020), user data was not properly encrypted. LinkedIn (2021) demonstrated a lack of strong API authentication. Meanwhile, in the SolarWinds (2020) case, software integrity was compromised due to the injection of malicious code in system updates, highlighting vulnerabilities in the IT supply chain.

Organizational responses are generally reactive, such as fixing system configurations or confirming breaches after incidents occur. However, the responses often lack adequate transparency or long-term mitigation strategies. This pattern reflects limitations in the implementation of proactive controls in line with the principles of confidentiality, integrity, and availability (CIA Triad) and is not yet fully integrated with international frameworks such as ISO/IEC and NIST.

Based on the observed vulnerabilities, the following mitigation strategies are formulated using the CIA Triad security framework and aligned with ISO/IEC 27002 and NIST SP 800-12 Rev. 1. Each strategy addresses confidentiality, integrity, and availability through a layered control model:

1. Confidentiality is strengthened through technical controls such as modern encryption protocols (e.g., TL 1.3, end-to-end encryption) and access governance at the API level, supported by administrative controls like identity-based access policies and role-based permission structures.
2. Integrity is addressed through technical mechanisms such as blockchain-based record verification and cryptographic hash functions (e.g., SHA-256), combined with administrative controls such as secure software development practices and audit logging (audit trails), as demonstrated in the SolarWinds case.
3. Availability is improved by using technical methods like API throttling and automatic failover mechanisms, physical controls such as backup systems, and administrative measures such as incident response planning and DDoS attack mitigation policies.
4. This study creates a clear and organized security framework that organizations can follow to lower risk and improve their ability to handle cyber threats by linking each risk-reduction strategy to the CIA Triad dimensions and ISO/NIST control categories.

Discussion

Mapping Technical Vulnerabilities to CIA Triad

This section organizes the four case studies of data breaches according to the CIA Triad (Confidentiality, Integrity, and Availability) to show how this framework can help assess security weaknesses and responses to regulations in each data breach case. Figure 4 highlights recurring security weaknesses from four major data breaches: insufficient encryption (Tokopedia), weak API protection (LinkedIn and Facebook), and compromised supply chain integrity (SolarWinds). These findings align with the CIA Triad: Confidentiality was compromised due to public data exposure and weak access controls. Integrity is threatened by compromised software updates. Availability is impacted by delayed responses and service disruptions. This pattern also indicates broader systemic issues such as delayed threat detection, lack of transparency, and inconsistent application of security standards. In response to the weaknesses, the recommended mitigation strategies include:

1. Tokopedia: Enhancing data encryption during both storage and transmission
2. Facebook: Restricting API access based on user identity and enforcing stricter API management policies
3. LinkedIn: Strengthening API authentication and applying AI-based anomaly detection
4. SolarWinds: Implementing AI-driven supply chain monitoring and conducting regular software code reviews.

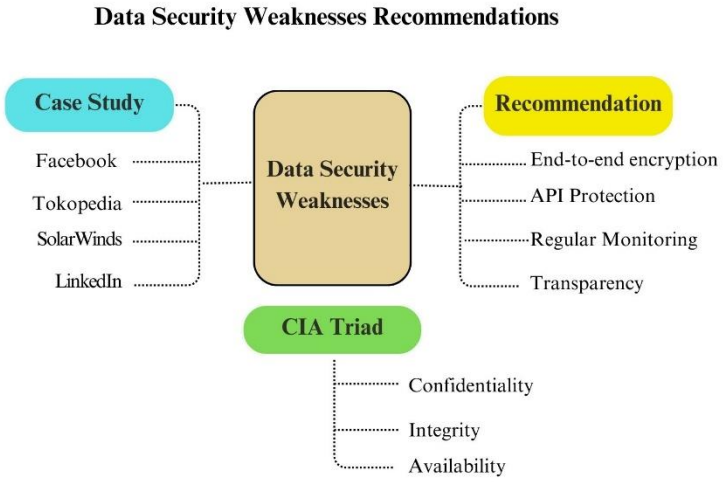

Figure 4. Data Security Weaknesses with CIA Triad

These recommendations align with the CIA Triad framework, underscoring the need to enhance confidentiality, integrity, and availability in a coordinated manner. From a regulatory perspective, the CIA Triad is also relevant to global compliance mandates: confidentiality relates to Article 32 of the GDPR and the principle of data minimization in Article 5; integrity supports accountability as regulated in Indonesia's PDP Law and China's PIPL; and availability reflects the importance of service continuity and incident reporting procedures.

Although legal frameworks such as the GDPR, PDP Law, and PIPL are in place, this study shows that their implementation still faces challenges such as enforcement gaps and differences in reporting standards. Therefore, the CIA Triad serves not only as a technical classification tool but also as a framework for evaluating readiness and compliance in the context of cross-jurisdictional data protection.

Strategic Recommendations and Preventive Measures

Table 1 presents a structured analysis of four high-profile data breaches: Facebook (2019), LinkedIn (2021), Tokopedia (2020), and SolarWinds (2020), using the CIA Triad dimensions: Confidentiality, Integrity, and Availability. Each case is evaluated based on the presence and effectiveness of technical,

administrative, and physical controls, drawing from international standards such as ISO/IEC and NIST SP 800-12 Rev. 1.

The findings indicate that confidentiality breaches are the most widespread, particularly those resulting from insufficient API controls and a lack of encryption mechanisms, as seen in the Facebook and LinkedIn cases. These weaknesses allowed for unauthorized access and mass data scraping, underscoring identity and access management vulnerabilities.

Table 1. CIA Triad Analysis with ISO/NIST Controls and Implementation Gaps

CIA Dimension	Case	Technical Control	Administrative Control	Physical Control	Implementation Gap
Confidentiality	Facebook (2019)	Transport encryption (TLS)	Access control policies	Perimeter secured, but restricted	No restrictions on API for importing contacts
	LinkedIn	API access tokens	API security protocols	No explicit physical security record	Mass data scraping of user data
Integrity	Tokopedia	End-to-end encryption	Data handling guidelines	Server access restricted, but standard	Lack of encryption for user data
	SolarWinds	Cryptographic hashing	Software integrity checks	Physical security measures	Service outages in response to breach
Availability	SolarWinds	Cloud-based load balancing	DDOS mitigation planning	Backup power systems	Service outages in response to breach

In the case of integrity, the SolarWinds incident demonstrates how compromised software integrity and supply chain trust can lead to system-wide infiltration despite the presence of cryptographic hashing and physical security controls. Similar to Tokopedia, it highlights how inadequate encryption standards and data handling guidelines weakened the integrity of stored user information.

While availability was less directly affected in some scraping-related events (e.g., LinkedIn), the SolarWinds attack significantly disrupted service delivery, revealing shortcomings in load balancing, DDOS mitigation planning, and backup systems. These gaps underscore the need for more resilient infrastructure, especially in critical service providers.

Furthermore, the analysis also reveals that beyond technical shortcomings, these cases expose systemic gaps in regulatory enforcement and breach transparency, for example, despite the existence of frameworks like GDPR, PIPL, and Indonesia's PDP Law, inconsistent implementation and weak enforcement.

Involving Models in Strengthening CIA Principles

The CIA Triad, augmented by ISO and NIST standards, established a foundational framework for categorizing and addressing security vulnerabilities. However, its conventional implementation often centers on reactive measures. In contrast, Zero Trust Architecture (ZTA) offers a proactive approach that assumes breaches by default, continuously verifies identities, and enforces least privilege access. This section explores how ZTA principles could have mitigated the key vulnerabilities identified in the review of data breach cases.

For instance, in the Facebook incident, where public profile data was harvested through the contact importer API, ZTA's enforcement of strict access limitations and continuous verification could have constrained data exposure by implementing request thresholds and detecting abnormal access patterns. In the LinkedIn case, similar protection might have been achieved through real-time identity verification and adaptive, risk-based access controls to detect and limit non-human interaction patterns.

During the Tokopedia breach, when user data was compromised, ZTA would require device authentication and strong endpoint protection prior to granting data-level access—potentially preventing large-scale internal downloads. Meanwhile, the SolarWinds compromise illustrates how ZTA's assume-breach model necessitates validation of all software updates, including internal ones, through code integrity checks and user-aware access controls, thereby impeding lateral movement by attackers. Overall, ZTA signifies a paradigm shift from static perimeter defense to dynamic, continuous protection informed by the user's device and application environment.

Complementing this approach, threat modeling frameworks such as STRIDE, which covers spoofing, tampering, repudiation, information disclosure, denial of service, and privilege escalation, provide a structured way to identify vulnerabilities early in the system design process. STRIDE reinforces Zero Trust by enabling organizations to anticipate threat vectors aligned with the dimensions of the CIA Triad.

Comparative Analysis with Previous Studies

This study offers a different contribution from previous research on large-scale data breaches. Research on Facebook, such as by Isaak & Hanna (2018), Hinds (2020), and Foecking (2021), focuses more on privacy issues, public perception, and market reactions, without systematically discussing the classification of technological risks. Studies on Tokopedia by Indrawati & Putri (2021) and Wibowo (2024) highlight that customer trust and national policies do not evaluate technical vulnerabilities. In the case of LinkedIn, Gibson (2021) discusses API scraping vulnerabilities, but their approach is limited to technical aspects and ignores regulatory frameworks. For SolarWinds, analyses by Lazarovitz (2021), Sterle & Bhunia (2021), Yang (2022), and Bulgurcu & Mashatan (2024) address technical and institutional aspects but have not yet adopted an integrated approach that incorporates theory, security standards, and cross-national regulations.

This study complements previous research by integrating technical vulnerability analysis based on the CIA Triad principles and risk classification using ISO/NIST standards. Additionally, this approach simultaneously compares global data protection regulations such as GDPR, PIPL, and PDP Law, unlike partial approaches that focus on technical, institutional, or policy aspects separately, by unifying technical, governance, and policy dimensions across jurisdictions within a single evaluative framework. As a result, this research expands understanding of the dynamics of global data breaches. It offers a mitigating model applicable to cross-border policy and security system development.

Implications

Theoretical Contributions

This study contributes theoretically to the development of a cybersecurity framework by demonstrating the potential effectiveness of the CIA Triad approach integrated with control standards such as ISO/IEC 27002 and NIST SP 800-12 Rev. 1. By applying it to four large-scale data breach cases, this approach offers a practical initial framework for identifying and assessing vulnerabilities based on the dimensions

of confidentiality, integrity, and availability. The study also proposes using proactive defense models such as the Zero Trust Architecture and STRIDE threat modeling as relevant advanced approaches to strengthen information security systems. It opens the door for further research to empirically test these models' effectiveness.

Previous studies on Facebook have generally focused on public perception, privacy, and market impact, while analyses of LinkedIn have emphasized technical vulnerabilities such as API scraping. Studies on Tokopedia have highlighted customer trust and the national policy context, while studies related to SolarWinds have discussed institutional barriers and security system design. However, these approaches tend to be limited to one technical, institutional, or regulatory dimension. This research complements the discourse by integrating CIA Triad-based analysis, ISO/NIST standard risk classification, and cross-regulatory comparisons such as GDPR, PIPL, and PDP Law. The main theoretical contribution of this study lies in developing a holistic and cross-domain evaluative framework that can be used to assess and mitigate data security risks in increasingly complex and fragmented global digital systems.

Practical Contributions

In practical terms, the findings of this study provide strategic guidance for organizations in improving their information security systems, particularly for entities that manage sensitive data across systems and jurisdictions. This approach can be used to develop mitigation measures such as strengthening encryption, managing API access, and monitoring digital supply chain risks. Findings from the case studies reveal common weaknesses in confidentiality and integrity aspects that require reinforcement with technical controls and consistent internal audits. Implementing measurable, risk-based minimum security standards is essential to promote digital resilience while supporting compliance with applicable regulations.

Policy Implications

The findings in this study also have policy relevance, especially in the context of strengthening the law enforcement system for cross-jurisdictional data breaches. The inconsistency in the application of regulations such as GDPR, PIPL, and PDP Law indicates the need for synchronization that can strengthen accountability across jurisdictions and improve the protection of user rights in the global digital ecosystem.

Conclusion

The analysis identified persistent security issues across four high-profile cases: lack of encryption (Tokopedia), weak API access control (Facebook and LinkedIn), and supply chain integrity failures (SolarWinds). These findings highlight a recurring neglect of fundamental cybersecurity principles, particularly data confidentiality and integrity. CIA Triad-based analysis confirms that confidentiality is the most vulnerable dimension, integrity is largely dependent on third-party trust, and while availability is not always compromised, breaches continue to affect service continuity and user trust. Additional issues, such as delayed detection, lack of transparency, and inconsistent implementation of standards, emphasize the need for systemic improvements in information security management.

This study uses the CIA Triad framework, supported by ISO/IEC 27002 and NIST SP 800-12 Rev. 1 standards, to identify technical, administrative, and physical weaknesses in four major incidents: Facebook, Tokopedia, LinkedIn, and SolarWinds. The application of this framework revealed that confidentiality breaches were the most prevalent, mainly due to weak API controls and insufficient encryption in three out of four cases. In the SolarWinds case, the integrity and availability were significantly affected due to supply chain compromises and post-attack service disruptions. This analysis demonstrates the value of integrating the CIA Triad with ISO/NIST controls to systematically identify critical weaknesses and corresponding mitigation strategies. It also recommends the future application of Zero Trust Architecture and STRIDE threat modeling to enhance proactive security measures by enabling continuous monitoring and early threat detection.

Although regulations such as GDPR, Indonesia's PDP Law, and China's PIPL provide comprehensive data protection frameworks, their real-world implementation in large-scale breach scenarios remains inconsistent and limited. While companies like Facebook have faced substantial penalties, regulatory enforcement overall has failed to ensure deterrence or cross-jurisdictional compliance. Ongoing challenges include a lack of transparency, delayed reporting, and insufficient legal coordination. These findings suggest the urgent need to reinforce implementation mechanisms, harmonize international data policies, and demand greater accountability from digital service providers.

The study is limited by its descriptive approach and narrow focus on four cases without empirical testing of mitigation strategies. Future research could adopt experimental designs to evaluate technical effectiveness and explore the role of emerging technologies, such as artificial intelligence and blockchain, in fostering cross-sector cyber resilience. Research could also develop security assessment models for public cloud environments, monitor the long-term impact of cross-border incident reporting mandates, and examine how evolving regulatory frameworks influence cybersecurity improvements in critical sectors like fintech and digital health. By addressing the fragmented nature of prior studies, this integrative approach aims to open new avenues for evaluating and mitigating data breach risks across platforms and jurisdictions.

References

Abbo, I., & Tchomte, N. D. (2024). Feature engineering and computer vision for cybersecurity. In Advances in information security, privacy, and ethics book series (pp. 155–174).

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*, *122*, 102911.

Adams, J., & Liu, M. (2022). Impact of User Experience and Comprehension on Awareness Training. *AMCIS 2022 Proceedings*.

Agustini, P. (2021). *Seputar Kebocoran Data Pribadi di Facebook dan Hoaks*. Kominfo. https://aptika.kominfo.go.id/2021/04/Seputar-Kebocoran-Data-Pribadi-Di-Facebook-Dan-Hoaks/

Ahmed, A., Awais, M., Siraj, M., & Umar, M. (2023). Enhancing Cybersecurity with Trust-Based Machine Learning: A Defense against DDoS and Packet Suppression Attacks. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, *23*, 262–268.

Ajagbe, S. A., Oyediran, M. O., Nayyar, A., Awokola, J. A., & Al-Amri, J. F. (2022). P-ACOHONEYBEE: A Novel Load Balancer for Cloud Computing Using Mathematical Approach. *Computers, Materials and Continua*, *73*(1), 1943–1959.

Alekseenko, A. P. (2022). Privacy, Data Protection, and Public Interest Considerations for Fintech. In H.-Y. Chen, P. Jenweeranon, & N. Alam (Eds.), *Global Perspectives in FinTech* (pp. 25–49). Springer International Publishing.

Alguliyev, R., Nabiyev, B., & Dashdamirova, K. (2023). CTI Challenges and Perspectives as a Comprehensive Approach to Cyber Resilience. *2023 5th International Conference on Problems of Cybernetics and Informatics (PCI)*, 1–5.

Alshahrani, H. M., Alotaibi, S. S., Ansari, M. T. J., Asiri, M. M., Agrawal, A., Khan, R. A., Mohsen, H., & Hilal, A. M. (2022). Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Applied Sciences*, *12*(12), 5911.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531.

Anwar, M., & Gill, A. (2020). Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. *ACIS 2020 Proceedings*.

Arunkumar, B., & Kousalya, G. (2018). Analysis of AES-GCM Cipher Suites in TLS. In S. M. Thampi,

S. Mitra, J. Mukhopadhyay, K.-C. Li, A. P. James, & S. Berretti (Eds.), *Intelligent Systems Technologies and Applications* (Vol. 683, pp. 102–111). Springer International Publishing.

Ayyagari, R. (2020). Data Breaches and Carding. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 939–959). Springer International Publishing.

Bajaj, K. (2012). Promoting Data Protection Standards through Contracts: The Case of the Data Security Council of India. *Review of Policy Research*, *29*(1), 131–139.

Bansal, G. (2018). Data Breaches and Trust Rebuilding: Moderating Impact of Signaling of Corporate Social Responsibility. In F. F.-H. Nah & B. S. Xiao (Eds.), *HCI in Business, Government, and Organizations* (Vol. 10923, pp. 253–261). Springer International Publishing.

Bendix, W., & MacKay, J. (2022). Fox in the henhouse: The delegation of regulatory and privacy enforcement to big tech. *International Journal of Law and Information Technology*, *30*(2), 115–134.

Ben-Nakhi, A. A., El-Barr, M. A., & Qureshi, K. (2023, December 1). *Threat Modeling of IoT-based Smart Home Systems. | EBSCOhost*.

Berki, E., Valtanen, J., Chaudhary, S., & Li, L. (2018). *The Need for Multi-Disciplinary Approaches and Multi-Level Knowledge for Cybersecurity Professionals*. IGI Global Scientific Publishing.

Bhardwaj, A. (2024). *Insecure Digital Frontiers: Navigating the Global Cybersecurity Landscape* (1st ed.). CRC Press.

Bobbert, Y., & Timmermans, T. (2023). How Zero Trust as a Service (ZTaaS) Reduces the Cost of a Breach: A Conceptual Approach to Reduce the Cost of a Data Breach. In K. Arai (Ed.), *Proceedings of the Future Technologies Conference (FTC) 2023, Volume 4* (Vol. 816, pp. 433–454). Springer Nature Switzerland.

Botha, J., Grobler, M. M., & Eloff, M. M. (2017). *Global Data Breaches Responsible for the Disclosure of Personal Information: 2015 & 2016*. *0*, 63–72.

Buckley, G., Caulfield, T., & Becker, I. (2022). "It may be a pain in the backside but..." Insights into the resilience of business after GDPR. *Proceedings of the 2022 New Security Paradigms Workshop*, 21–34.

Bulgurcu, B., & Mashatan, A. (Atty). (2024). *Environmental Factors that Hinder an Organization's Ability to Learn from Cyber Incidents: A Case Study on SolarWinds*. Hawaii International Conference on System Sciences.

Campbell, B. (2020). *The Definitive Guide to AWS Infrastructure Automation: Craft Infrastructure-as-Code Solutions*. Apress.

Carroll, D. R. (2021). Cambridge Analytica. In G. D. Rawnsley, Y. Ma, & K. Pothong (Eds.), *Research Handbook on Political Propaganda*. Edward Elgar Publishing.

Chin, Y.-C., & Zhao, J. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws*, *11*(4), 63.

Clark, M. (2021, April 6). *The facts on news reports about Facebook data*. Meta. https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

CNBC. (2020). *Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia*. https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia

CNN Indonesia. (2021). *Data Pengguna Linkedin Bocor, Dijual di Dark Web*. https://www.cnnindonesia.com/teknologi/20210630130302-185-661303/data-pengguna-linkedin-bocor-dijual-di-dark-web

Cybersecurity and Infrastructure Security Agency. (2021). *ED 21-01: Mitigate SolarWinds Orion code*

compromise (Cybersecurity directive). US Department of Homeland Security. https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

Dhanushkodi, K., & Thejas, S. (2024). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. *IEEE Access*, *12*, 173127–173136.

Das, P., Asif, Md. R. A., Jahan, S., Ahmed, K., Bui, F. M., & Khondoker, R. (2024). STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. *Vehicles*, *6*(3), 1140–1163.

De Oliveira Albuquerque, R., Villalba, L., Orozco, A., Buiati, F., & Kim, T.-H. (2014). A Layered Trust Information Security Architecture. *Sensors*, *14*(12), 22754–22772.

Dennis, A., Jones, R., Kildare, D., & Barclay, C. (2014). Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica. *The Electronic Journal of Information Systems In Developing Countries*, *62*(1), 1–18.

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. *Lecture Notes in Computer Science*, 238–257.

Fauzi, R., & Sembiring, J. (2023). A Review on Information Security Risk Assessment of Smart Systems: Risk Landscape, Challenges, and Prospective Methods. *2023 10th International Conference on ICT for Smart Society (ICISS)*, 1–6.

Federal Trade Commission. (2019). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Feys, M. (Maggie), Swanson, J. W., Carreiro, P. M., & Lafever, G. (2023). Technical controls that protect data when in use and prevent misuse. *Journal of Data Protection & Privacy*, *5*(3), 281.

Firmansyah, B. (2024). Cybersecurity Fundamentals: In B. Gupta (Ed.), *Advances in Computational Intelligence and Robotics* (pp. 280–320). IGI Global.

Fleury-Charles, A., Chowdhury, M. M., & Rifat, N. (2022). Data Breaches: Vulnerable Privacy. *2022 IEEE International Conference on Electro Information Technology (eIT)*, 538–543.

Foecking, N., Wang, M., & Huynh, T. L. D. (2021). How do investors react to the data breaches news? Empirical evidence from Facebook Inc. during the years 2016–2019. *Technology in Society*, *67*, 101717.

Fritz, J., & Kaefer, F. (2017). The Rise of the Mega Breach and What Can Be Done About It. *Journal of Applied Security Research*, *12*(3), 392–406.

Gibson, B., Townes, S., Lewis, D., & Bhunia, S. (2021). Vulnerability in Massive API Scraping: 2021 LinkedIn Data Breach. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 777–782.

Goluboff, M. (2015). AES vs SSL/TLS: Encryption for the internet of things. *Electronic Products*, *57*(7).

Gootman, S. (2016). OPM Hack: The Most Dangerous Threat to the Federal Government Today. *Journal of Applied Security Research*, *11*(4), 517–525.

Government of Indonesia. (2022). *Personal Data Protection Law*. *016999*, 457–483.

Guo, G., Yang, T., & Liu, Y. (2018). Search engine based proper privacy protection scheme. *IEEE Access*, *6*, 78551–78558.

Guo, J., Xu, M., Yuan, H., Zeng, J., & Zhang, J. (2022). Introduction of Endogenous Security of Zero Trust Model. *Journal of Zhengzhou University - Natural Science*, *54*(6), 51–58.

Hamid, S., & Huda, M. N. (2025). Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. *Social Sciences & Humanities Open*, *11*, 101234.

Hamidi, M. S., & Singh, B. (2024). Designing a Novel Cybersecurity Framework to Prevent Cyber-Attacks with Reference to Least Developing Countries. *Nanotechnology Perceptions*, *20*(S3), 159–165.

Hasibovic, A. C., & Tanovic, A. (2024). Review of ISO 9001:2015 and ISO 27001:2013 Implementation in Financial Institution – Case Study. *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, 1520–1525.

Heimes, R. (2016). Global InfoSec and Breach Standards. *IEEE Security & Privacy*, *14*(5), 68–72.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 102498.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242–260.

Hossain, M. I., & Hasan, R. (2023). Improving Security Practices in Health Information Systems with STRIDE Threat Modeling. *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, 1–6.

Hossain, M. M., & Hong, Y. A. (2019). Trends and characteristics of protected health information breaches in the United States. *AMIA ... Annual Symposium Proceedings. AMIA Symposium*, *2019*, 1081–1090.

Ilyas, M., Akal, M., & Althebyan, Q. (2024). Maturity Model for Corporate Sector Based on Zero Trust Adoption. *2024 International Conference on Engineering and Emerging Technologies (ICEET)*, 1–7.

Indrawati, & Putri, N. P. O. I. Y. (2021). Indonesian Marketplace Trust Analysis Using Text Mining: A Case of Tokopedia. *2021 International Conference Advancement in Data Science, E-Learning and Information Systems (ICADEIS)*, 1–6.

Information Commissioner's Office (2019). *Investigation into data analytics for political purposes*. https://icoumbraco.azurewebsites.net/action-weve-taken/investigation-into-data-analytics-for-political-purposes/

Irungu, J., & Girma, A. (2023). Cybersecurity and Electoral Processes. An Analysis of Block Chain Enabled Biometric Voter System and Risk Control in Kenya's 2022 Electoral Process and the United States Election System Infrastructure. *International Conference on ICT Convergence*, 687–694.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59.

Jacobs, P., Solms, S. V., & Grobler, M. (2016). E-CMIRC: Towards a model for the integration of services between SOCs and CSIRTs. *Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016*, 350–360.

Jonnala, A., Ampani, R., Abbasi, D. F., Alsadoon, A., & Prasad, P. W. C. (2023). Data Security Risk Mitigation in the Cloud Through Virtual Machine Monitoring. In S. C. Mukhopadhyay, S. M. N. A. Senanayake, & P. W. C. Withana (Eds.), *Innovative Technologies in Intelligent Systems and Industrial Applications* (Vol. 1029, pp. 227–238). Springer Nature Switzerland.

Joseph, R. C. (2018). Data Breaches: Public Sector Perspectives. *IT Professional*, *20*(4), 57–64.

Joshi, K. P., Elluri, L., & Nagar, A. (2020). An Integrated Knowledge Graph to Automate Cloud Data Compliance. *IEEE Access*, *8*, 148541–148555.

Juma'h, A. H., & Alnsour, Y. (2021). How Do Investors Perceive the Materiality of Data Security Incidents: *Journal of Global Information Management*, *29*(6), 1–32.

Khare, P., & Raghuwanshi, V. (2024). Navigating Emerging AI Technologies and Future Trends in Cybersecurity and Forensics: In M. Omar & H. M. Zangana (Eds.), *Advances in Digital Crime, Forensics, and Cyber Terrorism* (pp. 321–346). IGI Global.

Kroculick, J. B. (2024). Zero trust decision analysis for next generation networks. In B. T. Wysocki, M. Blowers, & R. Bharadwaj (Eds.), *Disruptive Technologies in Information Sciences VIII* (p. 26). SPIE.

Kucharavy, A., Plancherel, O., Mulder, V., Mermoud, A., & Lenders, V. (Eds.). (2024). *Large Language Models in Cybersecurity: Threats, Exposure and Mitigation*. Springer Nature Switzerland.

Kumar, J., & Ranganathan, G. (2023). Malware Attack Detection in Large Scale Networks using the Ensemble Deep Restricted Boltzmann Machine. *Engineering, Technology & Applied Science Research*, *13*(5), 11773–11778.

Lazarovitz, L. (2021). Deconstructing the SolarWinds breach. *Computer Fraud & Security*, *2021*(6), 17–19.

Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2025). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The Electronic Journal of Information Systems in Developing Countries*, *91*(1), e12350.

Lee, N. (2021). *Facebook Nation: Total Information Awareness*. Springer New York.

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), 270.

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1), 5536763.

LinkedIn Corporate Communications. (2021). *An update on report of scraped data*. https://news.linkedin.com/2021/june/an-update-from-linkedin

Liu, J. (2022). Towards a Global Regulatory Framework for Cross-Border Data Flows —Fundamental Concerns and the China's Approach. *Frontiers of Law in China*, *17*(3), 412–439.

Liu, J., Sengstschmid, U., & Yixuan, G. (2024). China's Cross-Border Data Flow Policies and Implications for Investments. In P. Cheung, L. Jingting, & U. Sengstschmid, *Data Governance and the Digital Economy in Asia* (1st ed., pp. 54–85). Routledge.

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1959.

Longras, A., Pereira, T., Carneiro, P., & Pinto, P. (2018). On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations. *2018 International Conference on Intelligent Systems (IS)*, 886–890.

Lugati, L. N., & Almeida, J. E. D. (2022). A LGPD e a construção de uma cultura de proteção de dados. *Revista de Direito*, *14*(1), 1–20.

Mackie, J., Taramonli, C., & Bird, R. (2017). Digital forensics and the GDPR: examining corporate readiness. *European Conference on Cyber Warfare and Security*.

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 117–122.

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., Sanchez, M. G., Grall, M., Hansen, M., & Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review*, *33*(4), 458–469.

Mary, A. D. (1999). Oracle Database Security. In *Handbook of Heterogeneous Networking*. Auerbach

Publications.

Marengo, F. (2020). Regulating data transfers through the international trade regime. *Manchester Journal of International Economic Law*, *17*(2), 266–297.

Mera-Amores, F., & Roa, H. N. (2024). Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance. In K. Arai (Ed.), *Advances in Information and Communication* (Vol. 920, pp. 197–207). Springer Nature Switzerland.

Mitrovic, Z., & Thakur, C. (2019). Positioning South Africa in the BRICS cybersecurity context: A strategic perspective. In L. L., van der W.-C. N., & van der W.-C. N. (Eds.), *14th International Conference on Cyber Warfare and Security, ICCWS 2019* (pp. 251–259). Academic Conferences and Publishing International Limited.

Mizrak, F., & Reyhan Akkartal, G. (2024). Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology. *Heliyon*, *10*(16), e35487.

Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. *Frontiers in Artificial Intelligence*, *8*, 1526221.

Mone, V., Abdulajonovich, S. M., Younas, A., & Petikam, S. (2024). Data Warfare and Creating a Global Legal and Regulatory Landscape: Challenges and Solutions. *International Journal of Legal Information*, *52*(2), 124–134.

New York State Department of Financial Services. (2015). *New York State Department of Financial Services*. https://www.dfs.ny.gov/

Nicko, J. C. (2021). *LinkedIn Data Leak – What We Can Do About It*. Scrubbed. https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/

Nijim, M., Goyal, A., Mishra, A., & Hicks, D. (2022). A Review of Nature-Inspired Artificial Intelligence and Machine Learning Methods for Cybersecurity Applications. In S. K. Shandilya, N. Wagner, V. B. Gupta, & A. K. Nagar (Eds.), *Advances in Nature-Inspired Cyber Security and Resilience* (pp. 109–118). Springer International Publishing.

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Peng, S., Sun, D., Zhu, L., Zhou, H., Zhang, X., & Cui, C. (2023). Enhancing Cross-Border Data Sharing in Blockchain Networks: A Compliance-Centric Approach Ensuring Anonymity and Traceability. *2023 3rd International Conference on Computer Science and Blockchain, CCSB 2023*, 200–204.

Pigola, A., & De Souza Meirelles, F. (2024). Unraveling trust management in cybersecurity: Insights from a systematic literature review. *Information Technology and Management*.

Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510–524.

Portalatin, M., Keskin, O., Malneedi, S., Raza, O., & Tatar, U. (2021). Data Analytics for Cyber Risk Analysis Utilizing Cyber Incident Datasets. *2021 Systems and Information Engineering Design Symposium (SIEDS)*, 1–6.

Poyraz, O. I., Bouazzaoui, S., Keskin, O., McShane, M., & Pinto, A. (2020). Cyber-Assets at Risk (CAR): The Cost of Personally Identifiable Information Data Breaches. *Proceedings of the 15th International Conference on Cyber Warfare and Security*.

Preethi, K. M., Ambika, M., Vickma, S., Megala, P., Yikram, D., & Santhoshkumar, S. P. (2024). Tech Guardians: Comprehensive Defense against Cyber Threats. *2nd International Conference on Sustainable Computing and Smart Systems, ICSCSS 2024 - Proceedings*, 549–551.

Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)*, 1–6.

Radanliev, P. (2024). Digital security by design. *Security Journal*, *37*(4), 1640–1679.

Rahman, Md. T., & Nemati, H. (2024). Impact of organizations' exposure in social media on the likelihood of a data breach. *AMCIS 2024 Proceedings*.

Rangrez, U. S., Qadri, S. A., Ashok Kumar, C., & Jothi Kumar, C. (2024). Cyber-Attack Defense System Enhanced by Artificial Intelligence. *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 1–5.

Riskinaswara, L. (2020, Mei). *Ada indikasi kebocoran data, Kominfo minta Tokopedia lakukan tiga hal ini*. Kominfo. https://aptika.kominfo.go.id/2020/05/ada-indikasi-kebocoran-data-kominfo-minta-tokopedia-lakukan-tiga-hal-ini/

Sadat, A., Lawelai, H., Younus, M., & Nurmandi, A. (2025). Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia. *Kasetsart Journal of Social Sciences*, *46*(1).

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, *20*(2), 163–180.

Schneider, G. (2022). Framing Accountability in Business-to-Government Data Sharing: The Gap Filling Role of Businesses' Corporate Digital Responsibility. *European Business Law Review*, *33*(6), 957–990.

Seaman, J. (2023). Zero Trust Security Strategies and Guideline. In *Advanced Sciences and Technologies for Security Applications* (pp. 149–168). Springer.

Shahul Ikram, N. A. H. (2024). Data Breaches Exit Strategy: a Comparative Analysis of Data Privacy Laws. *Malaysian Journal of Syariah and Law*, *12*(1), 135–147.

Share, A. (2021, June 30). *Reported LinkedIn data breach: 700 million users data exposed - Cybersecurity - Nixon Peabody Blog*. Nixon Peabody LLP. https://www.nixonpeabody.com/insights/articles/2021/06/30/reported-linkedin-data-breach-700-million-users-data-exposed

Sharma, R. C., & Zamfiroiu, A. (2023). Cybersecurity Threats and Vulnerabilities in the Metaverse. *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*, 1–7.

Sharma, S., Agrawal, S. S., & Kumar, S. A. (2024). Unlocking Cybersecurity Horizons: Exploring Cutting-Edge Technologies, Strategies, and Trends in the Dynamic Cyber Threat Landscape. *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 1–6.

Shelepov, A. (2022). Approaches of BRICS Countries to Data Regulation. *International Organisations Research Journal*, *17*(3), 212–234.

Shojaie, B., Federrath, H., & Saberi, I. (2016). *Getting the Full Benefits of the ISO 27001 to Develop an ISMS based on Organisations' InfoSec Culture*. International Symposium on Human Aspects of Information Security and Assurance.

Shoufan, A., & Damiani, E. (2017). On inter-Rater reliability of information security experts. *Journal of Information Security and Applications*, *37*, 101–111.

Simpson, W. R. (2022). Zero Trust Philosophy versus Architecture. In A. S.I., G. L., H. D.W.L., & K. A.M. (Eds.), *Lecture Notes in Engineering and Computer Science* (Vol. 2244, pp. 89–94). Newswood Limited.

Souabni, H., Benbrahim, H., & Amine, A. (2022). Secure Data Acces in Odoo System. *2022 8th International Conference on Optimization and Applications (ICOA)*, 1–5.

Sterle, L., & Bhunia, S. (2021). On SolarWinds Orion Platform Security Breach. *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 636–641.

Stottler, B. (2024). "Key" Tam: Giving Teeth to Federal Data Security Enforcement. *Minnesota Law Review*, *109*(2), 1003–1058.

Subhash, P., Qayyum, M., Likhitha Varsha, C., Mehernadh, K., Sruthi, J., & Nithin, A. (2024). A Security Framework for the Detection of Targeted Attacks Using Honeypot. In B. R. Devi, K. Kumar, M. Raju, K. S. Raju, & M. Sellathurai (Eds.), *Proceedings of Fifth International Conference on Computer and Communication Technologies* (Vol. 897, pp. 183–192). Springer Nature Singapore.

Sun, J. (2023). Facebook Cyber Security Evaluation. *SHS Web of Conferences*, *155*, 03013.

Tachepun, C., & Thammaboosadee, S. (2020). A Data Masking Guideline for Optimizing Insights and Privacy Under GDPR Compliance. *Proceedings of the 11th International Conference on Advances in Information Technology*, 1–9.

Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. *Information & Communications Technology Law*, *33*(3), 368–383.

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*, *95*(23), 6510–6522.

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics (Switzerland)*, *10*(22).

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 134–153.

Treacy, C., Loane, J., & McCaffery, F. (2020). A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In Y. M., C. P., N. J., & M. R. (Eds.), *Communications in Computer and Information Science: Vol. 1251 CCIS* (pp. 107–119). Springer.

US Government Accountability Office. (2022, February 8). *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*. https://www.gao.gov/products/gao-22-104746

Veit, R. D. (2022). Safeguarding Regional Data Protection Rights on the Global Internet—The European Approach Under the GDPR. In *Ius Gentium* (Vol. 96, pp. 445–484). Springer Science and Business Media B.V.

Verma, P. K., Singh, B., Shubham, P., Sharma, K., & Joshi, R. P. (2024). Evaluating the Effectiveness of Zero Trust Architecture in Protecting Against Advanced Persistent Threats. *Advances in Distributed Computing and Artificial Intelligence Journal*, *13*.

Vetrivel, S. C., Maheswari, R., & Saravanan, T. P. (2024). Industrial IOT: Security Threats and Counter Measures. In *Internet of Things: Vol. Part F2482* (pp. 403–425). Springer Science and Business Media Deutschland GmbH.

Viswanathan, G., & Prabhu, P. J. (2021). A hybrid threat model for system-centric and attack-centric for effective security design in SDLC. *Web Intelligence*, *19*(1–2), 1–11.

Volchkova, E. (2019). Integrated information security and privacy management system. *Atas Da Conferencia Da Associacao Portuguesa de Sistemas de Informacao*.

Von Solms, S. (2019). Africa's contribution to academic research in cybersecurity: Review of scientific publication contributions and trends from 1998 to 2018. In L. L., van der W.-C. N., & van der W.-C. N. (Eds.), *14th International Conference on Cyber Warfare and Security, ICCWS 2019* (pp. 476–483). Academic Conferences and Publishing International Limited.

Wang, Q. (2024). An Exploration of the Challenges of Cross-border Data Flow for International Investment Law by Counting and Fuzzy Numerical Analysis Algorithms. *Applied Mathematics and Nonlinear Sciences*, *9*(1).

Wang, X., Mansour, S., & El-Said, M. (2022). Introducing Zero Trust in a Cybersecurity Course. *SIGITE 2022 - Proceedings of the 23rd Annual Conference on Information Technology Education*, 118–120.

Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, *10*(1).

Xu, W., Wang, S., & Zuo, X. (2025). Whose victory? A perspective on shifts in US-China cross-border data flow rules in the AI era. *Pacific Review*.

Yan, J. (2024). Data privacy regulation and cross-border e-commerce. *Empirica*, *51*(4), 913–927.

Yang, J., Lee, Y., & McDonald, A. P. (2022). SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies. In L. R. (Ed.), *Studies in Computational Intelligence: Vol. 1012 SCI* (pp. 43–58). Springer Science and Business Media Deutschland GmbH.

Zaguir, N. A., De Magalhaes, G. H., & De Mesquita Spinola, M. (2024). Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. *IEEE Access*, *12*, 81608–81630.

Zhelyazkova, A., Kaya, C., & Schrama, R. (2017). Notified and substantive compliance with EU law in enlarged Europe: evidence from four policy areas. *Journal of European Public Policy*, *24*(2), 216–238.

Zhuo, R., Huffaker, B., Claffy, K., & Greenstein, S. (2021). The impact of the General Data Protection Regulation on internet interconnection. *Telecommunications Policy*, *45*(2), 102083.

How to cite:

Lutfiah, R. N., & Sulaksono, T. (2025). Cross-Border Data Security: Analysis of High-Profile Violations and Mitigation Strategies. *Jurnal Sistem Informasi (Journal of Information System)*, *21*(2), 23–46.