SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 01 (2025), pp. 95-98
Research Article
doi: https://doi.org/10.70710/sitj.v2i1.37

Threats of Data Leakage in Military Security Systems In the Regional Military Command III/Siliwangi

Diana Indriyana[1,a,*], Budi Prasetyono[2], Aloysus Mado[3]

[1,2,3]Sekolah Tinggi Intelijen Negara, Bogor
[a]diana_indriyana@yahoo.com
*Corresponding author

Article Info
Received: 17-Jan-2025
Revised: 29-Jan-2025
Accepted: 31-Jan-2025

Keywords
Data Leakage; Military Security System; Threat

Abstract
This research investigates the threat of data leakage to the military security system in the Kodam III/Siliwangi region. While advancements in information technology have positively impacted society, they also bring the threat of cybercrime. The Indonesian government has responded by enacting the Personal Data Protection Law and strengthening inter-agency collaboration to prevent and address cybercrimes. The threat of data leakage in the Kodam III/Siliwangi region falls under non-physical and unconventional military threats, posing risks to national security and social stability.

1. Introduction

Information is a crucial asset, serving as knowledge for humans. According to the Indonesian Dictionary (KBBI, 2024), information is defined as notifications, news, or reports about something. Information is a resource with value, enabling individuals to accomplish tasks that would be impossible without it. As the adage states, "knowledge is power," meaning that knowledge grants individuals the ability to act and seize opportunities (Warner, 2011). The rapid development of information technology has led to an increase in global data and information transmission. While its benefits are undeniable, the risks and threats associated with the misuse of information technology have become increasingly complex. Organizations are more vulnerable to threats and attacks on information security originating from internal personnel activities or external hacker intrusions (Jouini, Rabai, & Aissa, 2014).

One major impact of such security breaches is data leakage. According to wartaekonomi.co.id, data leakage refers to the unauthorized transmission of data from within an organization to an external destination or recipient. This can occur electronically or physically through websites, emails, and mobile storage devices such as optical media, USB drives, and laptops (Wibowo, 2021). Data leakage also refers to situations where confidential or sensitive information becomes vulnerable to unauthorized access or exposure (Pertiwi et al., 2022). Sensitive data such as personal information, customer data, business secrets, and financial records are prime targets for digital criminals (Kurnianingrum, 2023). Numerous corporations and large organizations have suffered financially and reputationally due to data breaches. Individuals affected by data leaks may experience identity theft, financial fraud, or even physical security threats (Yudistira & Ramadani, 2023). Beyond individual harm, data leaks, particularly in military or intelligence contexts, pose significant risks to national security.

Data leakage can occur due to stolen or lost storage devices, insider threats, negligence, or unauthorized system access through hacking (BSSN, 2019). Data hacking involves individuals or groups attempting to access, steal, alter, or damage stored electronic data, with objectives ranging from data theft and system disruption to espionage. Data breaches in the military are severe threats as they can compromise national security and military operations. Military institutions worldwide are prime targets for cyberattacks by other states, terrorist groups, or cyber criminals with varying motivations. A breach of military technology or strategic plans can erode a nation's competitive edge, disrupt tactical operations and communications, and even escalate physical conflicts (Singer & Friedman, 2014).

2. Research Methodology

This study employs a qualitative approach. According to Creswell, qualitative researchers recognize that reality is shaped by individuals involved in a research setting, with multiple realities existing in different situations. Data was collected through qualitative methods, including interviews and document studies, such as newspapers, literature, and journals related to military security system data leakage.

3. Findings and Discussion

Data leakage threats in Indonesia involve risks of exposing sensitive information such as personal, financial, or business data. These threats originate from cyberattacks, internal security breaches, or human factors such as negligence. Organizations mitigate these threats through security policies, encryption, and firewalls. The Indonesian government has enacted regulations such as Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) and the Ministry of Communication and Information Technology (Kominfo) regulations to safeguard personal data and national security. Today, information is regarded as "power," significantly influencing societal outcomes. With increasing dependence on information technology, risks are also escalating. Information technology is a "double-edged sword," as it contributes to human advancement while simultaneously serving as a tool for cybercrimes such as hacking, fraud, malware attacks, and espionage (Ekawati, 2018).

In 2022, cybercrimes in Indonesia saw a notable increase. According to e-MP Robinopsnal Bareskrim Polri data, 8,831 cybercrime cases were recorded between January and December 2022 (Polri, 2022). A prominent case was that of hacker Bjorka, who engaged in doxing—obtaining and disseminating personal information without authorization. Bjorka claimed to have accessed data from various government entities, including the Ministry of Law and Human Rights, PLN customer records, SIM card registration data, and election commission records (Yamananda, 2022). Military data breaches have historically occurred worldwide, involving both external and internal perpetrators. Three of the most significant cases include the Manhattan Project leak to the Soviet Union, leading to the nuclear arms race; the MiG-25 Foxbat fighter jet data leak from the Soviet Union to the United States; and the Iraq War Logs, where WikiLeaks exposed 400,000 classified U.S. and U.K. military documents from the Iraq conflict (2004-2009). Recently, a U.S. military base employee leaked classified documents on Discord.

Although Indonesia has not experienced direct military data leakage, the Ministry of Defense's website was hacked in 2022, potentially exposing sensitive data. Additionally, in August 2023, a case involving forged documents using Indonesian Army officers' data for illegal firearm purchases underscored the risks of data exposure. To prevent and counter military security data leakage, the Indonesian Armed Forces (TNI) have developed a multi-layered security system through Disinfolahta, focusing on personnel education, human resource development, secure data communication infrastructure, and specialized cyber defense procedures. Kodam III/Siliwangi has implemented Sisfopers, an information system storing military personnel data, incorporating VPNs and restricted IP access to enhance security.

4. Conclusion

Advancements in information technology have significantly benefited society, but they also present cybercrime challenges. The Indonesian government has responded by enforcing personal data protection laws, strengthening military security systems, and fostering inter-agency collaboration. Protecting personal data and cybersecurity is crucial in mitigating modern threats.

The threat of data leakage in the Kodam III/Siliwangi region arises when classified information is accessed by unauthorized parties, potentially compromising national security. This threat falls under non-physical and unconventional military threats. Unauthorized access to military information can erode trust and social stability. To counteract these risks, Kodam III/Siliwangi employs layered security measures, including Sisfopers and VPN restrictions. However, insider threats remain a concern. Preventative measures include regulatory enforcement, awareness campaigns, and legal enforcement under the Electronic Information and Transactions Law and Cyber Defense Guidelines. The significance of military data protection is reflected in intelligence technology utilization, such as Sisfopers, which incorporates high-quality hardware security measures. While effective, challenges persist, necessitating awareness of internal and external threats.

References

Alan F. Westin. 1967. *Privacy and Freedom*. New York: Atheneum

Bhatia, P., & Sehrawat, R. 2014. Type of Security Threats and its Prevention. IJSRDInternational *Journal for Scientific Research & Development*|, 2(08), 2321–0613. Retrieved from www.ijsrd.com

Bram Hazkiel, Ulfatun Fatma. 2022. Perlidungan Data Pribadi Warga Negara.

Cengage Learning.

Clarke,Richard A. dan Robert K.Knake. 2010. *Cyber War-The Next Threat to National Security and What to Do About It*.

Cornish, D. B., & Clarke, R. V. 2003. Opportunities, Precipitators, and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. *Crime Prevention Studies*, Vol.16, 41-96.

Dian Ekawati, Dian. 2018. "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan," *Jurnal Unes Law Review* 1, No. 2 (2018): 158

Grant, Robert M. 2016. *Contemporary Strategy Analysis: Text and Cases*. Ninth Edition. Chichester, West Sussex, United Kingdom: Wiley.

Habermas, Jürgen, Thomas Burger, and Frederick Lawrence. 1992. *The Structural Transformation of The Public Sphere: An Inquiry Into a Category of Bourgeois Society*. Cambridge (Mass.): The MIT press.

Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*. Vol.6. No. 1. Universitas Sebelas Maret.

Jemadu, Aleksius. 2007. 'Praktek-Praktek Intelijen Dan Pengawasan Demokratis: Pandangan Praktisi'. *Geneva Centre For The Democratic Control Of Armed Forces (Dcaf)* II: 23.

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. 2014. Classification of security threats in information systems. *Procedia Computer Science*, 32, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Kahn, David. 2001. 'An Historical Theory of Intelligence'. *Intelligence and National Security* 16(3): 79–92.

Konakalla, A., & Veeranki, B. 2013. Evolution of Security Attacks and Security Technology. *Ijcsmc*, 2(11), 270–276.

M Hasan Rumlus, Hartadi. 2020. Kebijakan Penanggulangan Pencurian Data.

M. Ade. 2022. Analisis RUU Perlindungan Data Pribadi.

M. Romli, Asep Syamsul. 2008. Kamus Jurnalistik. Bandung: Simbiosa Rekatama Media.

Pawar, M. V., & Anuradha, J. 2015. Network security and types of attacks in network. *Procedia Computer Science*, 48(C), 503–506. https://doi.org/10.1016/j.procs.2015.04.126

Pribadi dalam Media Elektronik. Volume 11, No. 2.

Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) BSSN. 2019. "Panduan Menghadapi Data Breach,".

Putri, Edelweiss Premaulidiani. 2022. Pentingnya Perlindungan Data di Indonesia Sebagai Upaya Tanggung Jawab Hukum Atas Kebocoran Data. Tesis. Magister Hukum. Universitas Islam Indonesia.

Segala, Saiful. 2013. Administrasi Pendidikan Kontemporer. Bandung: Alfabeta.

Silalahi, Putri Hasian dan Fiorella Angella Dameria. 2023. Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional*. Wajah Hukum* Volume 7(2), Oktober 2023, 614-627 Fakultas Hukum Universitas Batanghari Jambi ISSN 2598-604X (Online) | DOI 10.33087/wjh.v7i2.1244.

Singer, P. W., & Friedman, A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Warner J. Severin dan James W. Tankard, Jr..2011. *Teori Komunikasi: Sejarah, Metode, & Terapan Di dalam Media Massa*. Jakarta: Kencana Prenada Media Group

Whitman, M., & Mattord, H. 2017. *Management of Information Security*.