Factors Affecting Information System Security: Information Security, Cyber Threats and Attacks, Physical Security, and Information Technology (Literature Review)

Dwi Puji Lestari[1,*], Andika Luthfi Citra Tama[2], Siti Karlina[3], Achmad Sultan[4], Tarwoto[5]

[1,2,3,4,5] *Department of Information System, Universitas Amikom Purwokerto, Indonesia*

(Received: October 19, 2023; Revised: November 17, 2023; Accepted: December 19, 2023; Available online: January 7, 2024)

Abstract

Information systems are very important to support various organizational and individual activities. Therefore, information system security is an important issue in today's digital era, where it is very important to pay attention to the protection of sensitive data and information. This research aims to identify and analyze factors that influence information system security. These factors include information system security, cyber threats and attacks, physical security, and information technology. Each factor is thoroughly analyzed to understand its impact on information system security. The results of this research will help improve our understanding of the factors that influence information system security. These findings can be used as a basis for creating effective security policies in protecting the information assets owned by the organization. By understanding these things, organizations can optimize their security efforts against the ever-evolving security threats in today's digital world.

Keywords: Information System Security, Cyber Threats and Attacks, Physical Security, Information Technology, Qualitative and Literature Review

1. Introduction

In the continuously evolving digital era, information system security has become a critical concern for companies, organizations, and even individuals seeking to ensure the integrity, confidentiality, and availability of their data. The success and ease of leveraging information technology to enhance efficiency and productivity often hinge on the ability to secure information systems from the ever-evolving threats and cyber attacks.

Despite the conveniences offered by information systems, there are various criminal threats that must be addressed. These threats stem from criminals exploiting technological advancements to engage in activities such as data theft, information extortion, defamation, provocation, and propaganda with the intention of gaining benefits. These perpetrators employ various methods, including hacking, phishing, malware, and others, to achieve their objectives. Without effective protection or supervision of information system security, the likelihood of losing valuable information assets increases. Therefore, preventive measures and information system security need to be implemented to minimize the possibility of cyber attacks that could result in losses for individuals or specific groups [1].

Information security is defined as safeguarding information and information systems from unauthorized access, use, disclosure, operation, modification, or destruction to ensure confidentiality, integrity, and ease of use. Information system security consists of four areas: organization, people, processes, and technology [2]

The importance of information gives rise to the term information security. With an increasing number of information sources coming from the internet, information security involves computer and network technology as well as information and communication. The goal of information security is to maintain business continuity and reduce the

***Corresponding author: Dwi Puji Lestari (dwipuji988@gmail.com)**
DOI: https://doi.org/10.47738/ijiis.v7i1.193

 ISSN 2579-7069

impact of security incidents on business value by limiting the effects of security incidents. The implementation of information system security involves the application of various policies and measures to prevent, monitor, or handle any unauthorized access. Through this prevention, it is expected that critical data and assets cannot be accessed, damaged, or stolen by irresponsible parties [1].

Therefore, the main objective of this research is to identify the factors that can occur in information system security and also the influence of these information system threats.

2. Literature Review

2.1. Information System Security

Information system security is an effort to protect information assets from potential threats. Information security indirectly ensures business continuity, reduces risks, and can maximize investment returns [3]. Information security also encompasses data protection from attacks that can disrupt company or organizational operations, reduce risk exposure, and expedite decision-making processes regarding investments and commercial prospects[4]. Information system security safeguards all data and information sources from misuse by unauthorized individuals. The aim is to ensure that those accessing the data are genuinely authorized to access that data and information [5].

This information security is a crucial asset for an organization used in its strategy to create commercial value. Therefore, information security must be carefully considered at all levels of the organization[4]. Without adequate protection to maintain the security of a system, organizations risk losing their information assets [6]. According to Kang [8] there are four ways to describe the dimensions or indicators of information security: privacy as a human right, commodity, access limitations, and privacy to control personal information [3].

Information system security includes protection against the following aspects:

1) Confidentiality ensures the confidentiality of data or information and ensures that information can only be accessed by those authorized to access it.

2) Integrity ensures that data cannot be altered without permission from the authorized party and maintains the accuracy and integrity of the information held by the organization.

3) Availability guarantees that data will be available when needed and ensures that authorized users can access the information and data [8].

Therefore, it is essential for companies/organizations to implement security systems for data and information to address issues and challenges, both technical and non-technical, that can affect the performance of the system.

2.2. Cyber Threats and Attacks

Threats are actions or events that can endanger an organization, potentially resulting in various types of losses such as financial, employment, business opportunities, corporate reputation, or even bankruptcy [9].

Due to various factors, organizations are more vulnerable to network threats, information security attacks, and network attacks. Various threats or attacks have the potential to disrupt network or information system security, leading to leaks of personal and confidential data as well as a decline in company performance [6].

2.3. Physical Security

The implementation of information technology undoubtedly requires a comprehensive security system. Physical security is one of the security measures that must be considered. This security can encompass layout, equipment location, available IT equipment, security of the physical space itself, cable installation, migration and disposal of sensitive computers, as well as computer resource management. The physical storage of computers can prevent data loss or damage caused by physical environmental factors such as natural disasters and data theft [11].

2.4. Information Technology

 ISSN 2579-7069

Information technology is a category of resources that enables the creation, analysis, distribution, storage, and/or deletion of data and information. Hardware, software, databases, users/people, LAN, and WAN are dimensions or indicators of information technology [10].

Currently, the development of information technology is crucial for almost every organization to enhance the efficiency and effectiveness of business processes. Information systems evolve with the development of technology and require the ability to provide accurate and timely information. These systems are used to support various functions, even for gaining advantages and winning in business competition [11].

3. Research Methodology

This research aims to analyze factors influencing information system security, including information security, cyber threats and attacks, physical security, and information technology within the information system. In the writing of this scientific article, a qualitative method and literature review (Library Research) are employed. The article investigates theories and relationships concerning variables from journal articles, examining the impact of journals both offline in libraries and online sources from the internet [12]. Mendeley, Google Scholar, and other online platforms are used as literature reviews in qualitative research. The use of literature reviews should be consistent with methodological assumptions, ensuring an inductive approach rather than directing researcher questions. The primary reason for conducting qualitative research is its exploratory nature [2].

4. Result and Discussion

Based on the theoretical study and relevant previous research, the discussion in this article employs a literature review on Information Systems, focusing on the following aspects:

4.1. The Influence of Information Security on Information System Security

Information security affects the security of information systems because in the dimension or indicator of information security, efforts are made to protect information assets from threats. Therefore, information security indirectly influences information system security, helping to sustain business operations by reducing risks [13]. Information system security, security, and user security are essential to minimize the possibility of data leakage.

Information System Security strives to enhance the security of information systems by considering information security. Management processes are necessary to protect important and confidential information [14]. Information security is beneficial in safeguarding information from threats that could disrupt performance and achievement.

Information System Security has an impact when customers or consumers trust information security, elevating the organization's or company's information system security to a higher and more quality level (Informasi n.d.). Establishing organizational rules for the company is one way to manage data security effectively. Information security affects information system security, aligning with the research conducted by [15].

4.2. The Influence of Cyber Threats and Attacks on Information System Security

Information security significantly influences cyber threats and attacks. It is not merely about data protection but also involves a strategy comprising preventive, detection, and responsive actions against threats that can harm information integrity, confidentiality, and availability [16]. Information System Security in the context of cyber threats and attacks includes implementing various preventive measures, such as firewalls, antivirus software, and access controls, to reduce the likelihood of cyber attacks [17].

Organizations with robust security systems can thwart various types of threats before they can damage or access sensitive data.

In information security systems, Information System Security can implement effective early detection steps to identify potential threats by monitoring suspicious behavior, conducting log analysis, and using intrusion detection systems to detect signs of cyber attacks or suspicious behavior. Information System Security in information security systems can adopt rapid response measures where information security involves swift responses or fast response plans to address,

 ISSN 2579-7069

isolate affected systems, and recover data from backups. The potential damage caused by attacks decreases with the speed of the response.

4.3. The Influence of Physical Security on Information System Security

Physical security plays a crucial role in supporting the security of information systems. Threats to physical security can have a direct impact on the integrity, confidentiality, and availability of data and systems. Physical security provides a strong foundation for information system security. The integration of physical security and overall information security is necessary to protect data and systems from various threats that may arise from different sources.

Physical security significantly affects information system security by providing protection against threats that may arise from physical access to hardware and information technology infrastructure. Measures such as restricting access to server rooms, implementing visual surveillance through CCTV, and protecting against theft or physical damage form the basis for preventing unauthorized access or manipulation of hardware or IT infrastructure. Well-planned physical disaster preparedness, including data backups and recovery plans, can anticipate threats such as natural disasters or accidents. The loss or failure of hardware is greatly influenced by the management of the physical environment, such as temperature and humidity. By considering physical security comprehensively, organizations can ensure operational continuity and strengthen their information systems against various threats.

4.4. The Influence of Information Technology on Information System Security

Information technology is the combination of high-speed computation and communication for data, voice, and video. Information technology is the dimension or measure of technology. Advanced information technology consists of hardware, software, data, procedures, and people [18]. Information technology is a category of resources that enables the creation, analysis, distribution, storage, and/or deletion of data and information. Hardware, software, databases, local area networks (LAN), Wide Area Networks (WAN), and human or user devices (brainware) are dimensions or indicators of information technology.

To enhance Information System Security, effective management is essential. Information management includes all activities related to acquiring information, using it correctly, and eliminating useless data as quickly as possible. Improving information system security in information technology involves implementing strict security policies, such as identity management and tight access controls, regular updates of software and operating systems, the use of encryption technology to protect stored and transmitted data, and providing education to users about security risks. Additionally, it is necessary to ensure that intrusion detection systems and firewalls are configured correctly, and logs are regularly monitored to identify suspicious activities [19]. Some methods that can be used in information technology to enhance information system security include risk assessment, regularly assessing risks to identify potential threats and vulnerabilities in information systems. This aids in the development of security plans. Developing security policies involves clear and comprehensive security policies, which may include access regulations, passwords, monitoring, and other relevant security measures. User awareness training can also be conducted to educate users about good security practices, covering topics such as security policies, phishing threats, and reporting security incidents. Identity and access administration enhance access and identity management systems. Ensure that access rights are granted only as needed for the job and are terminated when no longer necessary. The last method involves updating operating systems and software; software, operating systems, and applications should always be updated to the latest version, typically with security fixes. Comprehensive efforts to maintain information system security and protect sensitive data from potential cyber threats include effective disaster recovery plans and routine security audits.

The Information Technology has an influence on Information System Security. When information technology is used wisely and effectively by consumers or customers, it enhances the quality of information system security, resulting in better and higher quality security behavior. Information Technology has an impact on Information System Security, consistent with the research conducted by Sudarso [20], and Putri Primawanti & Ali [21].

 ISSN 2579-7069

5. Conclusion

Based on a literature review in articles discussing factors influencing information system security, key elements include information security, cyber threats and attacks, physical security, and information technology within the information system. It is concluded that currently there are various methods employed to identify these factors affecting information system security, including information security, cyber threats and attacks, physical security, and information technology within the information system. By understanding these factors, namely information security, cyber threats and attacks, physical security, and information technology within the information system, measures can be implemented to secure and anticipate potential threats, ensuring information system security across various aspects.

Drawing from theories, relevant articles, and discussions, conclusions can be derived, leading to the formulation of hypotheses for further research:

1) Information security has an impact on information system security.

2) Cyber threats and attacks influence information system security.

3) Physical security affects information system security.

4) Information technology has an impact on information system security.

6. Declarations

6.1. Author Contributions

Conceptualization: D.P.L. and A.L.C.T.; Methodology: A.L.C.T.; Software: D.P.L.; Validation: D.P.L. and A.L.C.T.; Formal Analysis: D.P.L. and A.L.C.T.; Investigation: S.K.; Resources: A.S.; Data Curation: S.K.; Writing Original Draft Preparation: S.K. and T.; Writing Review and Editing: S.K. and T.; Visualization: T.; All authors, D.P.L., A.L.C.T., S.K., A.S., T., have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

References

[1] B. Laila Alfila, A. Mukhlis, dan A. Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer*, vol. 3, no. 2, pp. 143–152, 2023.

[2] G. Prasetyaningrum, F. Nurmayanti, dan F. Azahra, "Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat (Literature Review Sim)," *J. Manaj. Pendidik. Dan Ilmu Sos.*, vol. 3, no. 2, pp. 520–529, 2022, doi: 10.38035/jmpis.v3i2.1115.

[3] E. Hamdani dan H. Ali, "Pengaruh Keamanan Informasi, Teknologi Informasi dan Network terhadap Security of Information," *Jurnal Siber Multi Disiplin*, vol. 1, no. 3, pp. 115-122, 2023.

[4] A. Renaldy et al., "Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan," *Jurnal Ilmu Multidisplin*, vol. 2, no. 1, pp. 15-22, 2023.

[5] J. Jessima et al., "ANCAMAN DENIAL OF SERVICE ATTACK DALAM EKSPLOITASI KEAMANAN SISTEM INFORMASI," *Unes Journal of Information System*, vol. 8, no. 1, pp. 009-019, 2023.

[6] A. Bustami dan S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review," *Unistek*, vol. 7, no. 2, pp. 59-70, 2020.

[7] T. E. Wijatmoko, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy," *Cyber Security dan Forensik Digital*, vol. 3, no. 1, pp. 1-6, 2020.

[8] Y. Kang, A. Yu, dan W. Zeng, "Development of a Model for Recognizing Cracks on Concrete Surfaces Using Digital Image Processing Techniques," *Int. J. Appl. Inf. Manag.*, vol. 3, no. 3, pp. 118–124, Sep. 2023.

[9] A. Suryaputra Paramita, Shalomeira, dan V. Winata, "A Comparative Study of Feature Selection Techniques in Machine Learning for Predicting Stock Market Trends," *J. Appl. Data Sci.*, vol. 4, no. 3, pp. 147–162, Aug. 2023.

[10] L. A. Saputra et al., "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," *Jurnal Pendidikan Siber Nusantara*, vol. 1, no. 2, pp. 58-66, 2023.

[11] S. Nurul, S. Anggrainy, dan S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review SIM)," *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, pp. 564-573, 2022.

[12] H. Yahya et al., "Analisis Keamanan Fisik Data Prodi Sistem Informasi UIN Sumatera Utara Medan Menggunakan Standar ISO 27001," *Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta*, vol. 2, no. 1, pp. 39-44, 2023.

[13] Y. M. K. Ardhana, "Keamanan Sistem Informasi Keamanan Sistem Informasi," *J. MEDIA Apl. ISSN 2086 - 972X Vol. 2, No. 2, Mei 2012*, vol. 2, no. 2, pp. 1–9, 2012.

[14] C. Sillaber, A. Mussmann, dan R. Breu, "Experience: Data and information quality challenges in governance, risk, and compliance management," *J. Data Inf. Qual.*, vol. 11, no. 2, 2019, doi: 10.1145/3297721.

[15] Paryati, "Keamanan Sistem Informasi," *Semin. Nas. Inform. 2008 (semnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, vol. 2008, no. semnasIF, pp. 379–386, 2008.

[16] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, pp. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

[17] C. Rahmawati, "Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0," *Semin. Nas. Sains Teknol. dan Inov. Indones. (SENASTINDO AAU)*, vol. 1, no. 1, pp. 299–306, 2019, [Online]. Available: https://aau.e-journal.id/senastindo/article/view/116.

[18] A. Kadir dan T. Wahyuni, "Pengenalan Teknologi Informasi," no. April, hal. 45, 2013.

[19] A. Sudarso, "Pemanfaatan Basis Data, Perangkat Lunak Dan Mesin Industri Dalam Meningkatkan Produksi Perusahaan (Literature Review Executive Support System (Ess) for Business)," *J. Manaj. Pendidik. Dan Ilmu Sos.*, vol. 3, no. 1, pp. 1–14, 2022, doi: 10.38035/jmpis.v3i1.838.

[20] E. Soesanto et al., "Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA)," *Student Res. J.*, vol. 1, no. 3, pp. 227–238, 2023, doi: 10.55606/srjyappi.v1i3.334.

[21] E. Putri Primawanti dan H. Ali, "Pengaruh Teknologi Informasi, Sistem Informasi Berbasis Web Dan Knowledge Management Terhadap Kinerja Karyawan (Literature Review Executive Support Sistem (Ess) for Business)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 3, pp. 267–285, 2022, doi: 10.31933/jemsi.v3i3.818.