Original Research Paper

Volume - 12 | Issue - 06 | June - 2022 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Computer Science

INFORMATION SECURITY IMPACT ON ECONOMY

Azhar Ushmani PhD in Information Technology, University of the Cumberlands

KEYWORDS :

The gradual technological advancement has increased security vulnerabilities as hackers target information systems. The diffusion and interaction in the digital platform open up loopholes creating security concerns that may compromise the business operation. Information security is important in defining policies and guidelines to help organizations combat security vulnerability. It comprises three main domains, including confidentiality, integrity, and availability. They act as the foundation for an organization to formulate comprehensive security infrastructures and protect the business interest. Information security has a positive and negative impact on the economy depending on how efficiently organizations protect critical infrastructures. Protecting data and information in the information system gives the organization an upper hand in generating guidelines to respond to any security concerns. Appropriate response strategies are important in minimizing security vulnerabilities to improve economic performance.

Domains of Information Security

Information Security defines strategic processes for organizations to formulate policies and guidelines to protect information and data. According to Al-Dhahri et al. (2017), Information Security gives the organization the procedures of protecting information and information asset against unauthorized access since it can negatively affect the business efficiency. Organizations can implement ISO 27000 comprising policies and guidelines helping organizations identify embedded security vulnerabilities and recommend appropriate response strategies. In the long run, organizations can increase their competitive advantage due to improved business efficiency and a good reputation in the competitive market. Consumers trust the organization with their information and are not worried that the company may lose sensitive data to cyber-attacks. The improved business efficiency increases productivity and profitability, which improves economic performance. Therefore, acknowledging Information Security domains can help determine the security infrastructure and potential security vulnerabilities.

Confidentiality

Confidentiality is an aspect of Information Security defining strategies to prevent unauthorized disclosure of data or information. Organizations must maintain confidentiality by minimizing unauthorized access and placing effective access control policies. Sarker et al. (2021) reported that confidentiality eliminates unauthorized access giving the organization the control of all information and data. A confidentiality threat can target application services, system administrators, data theft, and database. Organizations must ensure effective security policies and guidelines prioritizing confidentiality by monitoring all individuals accessing the information internally or externally. The domain also acknowledged that personal information is private and only accessible and visible to the individual who needs it. For example, an entity can formulate access control policies that restrict information and data access within the enterprise based on roles and responsibilities. Only individuals with specific roles and responsibilities can access specific data, thus prioritizing confidentiality.

Integrity

Integrity is the second component of Information Security, acknowledging the consistency of protecting against unauthorized changes to the information. For example, Shen et al. (2018) supported data integrity for disseminating the information on the internet in the cloud-based platform to minimize information alteration. Protecting data over the internet is important in information security and creating an infrastructure to minimize unauthorized information changes. Only the individuals with the right authorization can access or change the information, hence optimizing security and data privacy. The principle of integrity increases data accuracy and reliability by minimizing incorrect modification, whether maliciously or accidentally.

Availability

Availability is the last aspect of Information Security, indicating the essence of availing the information when needed within an enterprise. Availability shows that the software system and data are always available when needed by the user old at a specific time. According to Yee and Zolkipli (2021), availability refers to providing authorized users access to related assets and information when they need them in the computer system. An organization has to ensure the information is available when needed to achieve a specific goal. It is a structure of information security guiding organizations toward system availability and data protection. Organizations can increase efficiency by developing effective Information Management processes and establishing interaction with the consumer. It protects the business interest and streamlines strategic goals and objectives.

Information Security and Economic Performance

Information Security positively impacts the economy by providing organizations with clear policies and guidelines to protect sensitive information. Minimizing the security vulnerabilities allows the organization to optimize its profitability and productivity due to the increasing customer base. Research by Steinbart et al. (2018) dictated that organizations can execute the internal audit and information security processes to determine the information security outcomes and focus on achieving the goals and objectives. Organizations can improve business efficiency and use the information to make adjustments to the existing security vulnerability. The internal audit process acknowledges the weaknesses in the existing information system providing relevant information to respond to impending security breaches. The framework is ideal for improving the economy since organizations can optimize efficiency by improving business processes. For example, it is easy to increase the customer base due to the good reputation of Information Security, thus improving sales and profitability. Good business operation positively influences economic development due to business expansion as it protects the information infrastructure.

However, inefficient security policies may negatively affect the organization. Companies have to develop policies and guidelines to respond to security vulnerabilities which increases the operational cost. Similarly, organizations experienced increased operational costs while responding to security vulnerabilities affecting the information systems. For example, in the case of a ransomware attack, the user must give a ransom to access the information. It negatively impacts the business operation since it ends up spending on unplanned expenditures. Cybercrime has become a major problem, and it is affecting the global economy due to the breaches in the digital platform. Indeed, Spremić and Šimunic (2018) predicted in 2018 that the global cost of responding to cyber security breaches would increase to $6 trillion by 2021, which would be double the total of security breaches in 2015. The projection is realistic since COVID-19 ushered in increased security vulnerabilities as people concentrated on digital platforms (Lallie et al., 2021). The analysis indicates the negative impact of cyber attacks that compromises economic performance in national and global forums. Therefore, without effective Information Security, there are instances of security vulnerabilities that may affect economic performance due to reduced business efficiency and profitability.

To sum up, information security is important in providing organizations with a sustainable security response mechanism. Information confidentiality, integrity, and availability are important drivers and have effective information in data management within an

enterprise. Sustainable security infrastructure promote improved business operations which positively influences economic development. Organizations increase profits and productivity, thus generating enough funds to increase investment, positively influencing economic development. However, the lack of effective information security guidelines can attract increased operational costs within an organization, thus affecting the economic performance. The increased technological advancement is attracting more security vulnerability that affects the company's profitability and also the global economy. Thus, information security is important in providing organizations with a reliable security framework to deal with security breaches.

REFERENCES

1. Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information security management system. International Journal of Computer Applications, 158(7), 29-33.
2. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.
3. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 1-18.
4. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2018). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. IEEE Transactions on Information Forensics and Security, 14(2), 331-346.
5. Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346).
6. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.
7. Yee, C. K., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT in Education, 8(2), 34-42.