Review Scientific Paper/Pregledni naučni rad UDC/UDK: 004.738.5.056:005.5
Paper Submitted/Rad primljen: 5. 2. 2023.
Paper Accepted/Rad prihvaćen: 22. 6. 2023.
DOI: 10.5937/SJEM2302048J

Značaj informacione bezbednosti za organizacije

Nenad Jevtić[1]*, Ibrahim Alhudaidi[2]

[1]Regional Center of the Ministry of Defense in Valjevo, nenad.jevtic@fim.rs
[2]Ministry of Foreign Affairs, United Arab Emirates, ialhudaidi@gmail.com

Apstrakt: Informaciona bezbednost predstavlja ključni aspekt poslovanja organizacija u današnjem digitalnom dobu. Ovaj rad ima za cilj da analizira značaj informacione bezbednosti za organizacije, istražujući njen uticaj na očuvanje integriteta, poverljivosti i dostupnosti podataka. Organizacije su sve više suočene sa kompleksnim izazovima u oblasti cyber pretnji, čime se naglašava nužnost implementacije efikasnih strategija informacione bezbednosti. Efikasna zaštita podataka ključna je za održavanje poverenja klijenata i partnera, smanjenje finansijskih gubitaka i očuvanje reputacije organizacije. Pored toga, informaciona bezbednost ima značajnu ulogu u očuvanju konkurentske prednosti, omogućavajući organizacijama da inoviraju bez straha od gubitka podataka ili povrede privatnosti. Bezbedna infrastruktura takođe pruža osnovu za usklađenost sa regulatornim zahtevima, čime se smanjuje rizik od pravnih posledica. Uzimajući u obzir brzi razvoj tehnologije i sve sofisticiranije cyber pretnje, organizacije se suočavanju sa stalnim izazovom prilagođavanja svojih bezbednosnih strategija. Edukacija zaposlenih postaje ključna komponenta celokupnog sistema informacione bezbednosti, a organizacije koje ulažu resurse u obuku i svest o bezbednosti imaju bolju sposobnost odgovora na potencijalne pretnje. Informaciona bezbednost postaje neophodan stub savremenog poslovanja, čuvajući organizacije od cyber rizika, unapređujući njihovu reputaciju i pružajući osnovu za dugoročni uspeh.

Keywords: informaciona bezbednost, cyber pretnje, zaštita podataka, edukacija o bezbednosti

The Importance of Information Security for Organizations

Abstract: Information security is a key aspect of organizations' operations in today's digital age. This paper aims to analyze the importance of information security for organizations, investigating its impact on preserving the integrity, confidentiality and availability of data. Organizations are increasingly faced with complex challenges in explaining cyber threats, which emphasizes the necessity of implementing effective information security strategies. Effective data protection is the key to maintaining the trust of clients and partners, reducing financial losses and preserving the organization's reputation. In addition, information security has a significant impact on maintaining a competitive advantage, allowing organizations to innovate without fear of data loss or privacy breaches. A secure infrastructure also provides a foundation for compliance with regulatory requirements, thereby reducing the risk of legal consequences. Considering the rapid development of technology and increasingly sophisticated cyber threats, organizations face the constant challenge of adapting their security strategies. Employee education is becoming a key component of the overall information security system, and organizations that invest resources in training and security awareness have a better ability to respond to potential threats. Information security is becoming a necessary pillar of modern business, protecting organizations from cyber risk, enhancing their reputation and providing the foundation for long-term success.

Keywords: information security, cyber threats, data protection, security education

1. Introduction

In today's digital ecosystem, where technological progress is fast and ubiquitous, information security takes on the role of a crucial component of organizations' operations, representing a key defense mechanism against cyber threats. This paper aims to highlight the necessity of information security for organizations, focusing on its impact on the integrity, confidentiality and availability of data. In a global context where technological progress is taking place quickly, organizations face the challenge of

adapting their security strategies in order to preserve their operational resources (Mitchell, 2014).
With the increasing digitization of the business environment, organizations face the constant challenge of adapting their security strategies in order to effectively respond to increasingly sophisticated cyber threats. In this sense, the first part of the paper is dedicated to considering the importance of a holistic approach to information security in organizations (Zimba & Chishimba, 2019). A holistic approach implies a comprehensive, integrated approach to security that includes technical, organizational and human aspects. Technical measures, such as encryption and firewalls, are important, but become more effective when combined with organizational policies and employee awareness.

The second part of the paper focuses on the importance of the implementation of information security in the context of preserving the trust and reputation of organizations, through the HAIS-Q model, which pays special attention to measuring employees' awareness of information security. Educated employees become the first line of defense against cyber threats, reducing the risk of human error.
Through these aspects, this paper wants to emphasize not only the importance of information security as a defense mechanism against cyber threats, but also to emphasize that this security is not limited to technical aspects only. People, as key factors, have a crucial role, and their awareness, education and engagement become key factors for preserving information security. Preserving the integrity, confidentiality and availability of data not only preserves organizational security, but becomes imperative for organizations that want to achieve sustainable growth and success in a dynamic and increasingly digitized business environment.

2. A holistic approach to information security in organizations

In today's business environment, the use of the Internet is becoming a key resource for business operations, almost equally as electricity (Harmon & Auseklis, 2009). This dependence on the digital environment brings increased risks to information security, making it necessary to preserve the integrity, confidentiality and availability of data. Experts agree that technology, although important, cannot alone guarantee information security, especially considering two basic categories of threats - internal and external (Skopik et al., 2016). Internal threats are becoming increasingly important in the field of information security. Carelessness, mistakes and omissions of users are often the source of incidents. The earlier emphasis on external threats has today been replaced by a more comprehensive approach that also includes the human factor. A holistic approach, encompassing technical, organizational and human aspects, becomes crucial for effective information security management. User behavior is a key factor in this context. The Internet, a network of great potential, is exposed to various threats. Human error, whether the result of carelessness or lack of training, is often the source of information security incidents. A holistic approach, which includes employee training, becomes necessary to preserve information security (Da Veiga et al., 2020). Organizations face the challenge of recognizing the importance of user behavior and human error in maintaining information security. Investing in employee education becomes key to reducing the risk of security incidents.

Technology, while necessary, is not sufficient. Integrating technical measures with policies, procedures and education enables comprehensive information security. As previously mentioned, information security incidents often result from human error, lack of awareness of potential threats, and lack of information security knowledge (Alavi et al., 2013). It is crucial to encourage and train employees so that they become aware of the information security policy. Increasing employee awareness of information security can significantly reduce the risk of incidents. Empirical research on organizational information security is still in its infancy. Automation of certain security procedures makes operational tasks easier for employees, but on the other hand, behaviors that imply user responsibilities are not solved exclusively by technology. Users' attitude toward information security, their perception of social norms, threat assessment, and level of self-efficacy become key factors influencing their information security behavior. A holistic approach to information security, which integrates technical measures with training, policies and procedures, is a key strategy for organizations striving to effectively manage information security. Investing in employee training, raising awareness of information security, and promoting positive attitudes toward information security are becoming imperative to preserve the integrity, confidentiality, and availability of data in modern digital business.

3. The importance of awareness of information security among employees and the way of its quantitative measurement through the HAIS-Q model

Defining information security awareness usually focuses on two key aspects, while the first of them focuses on employees' understanding of the importance of information security (Snyman & Kruger, 2021). Kruger (2010) defined information security awareness as "the degree or extent to which each staff member understands the importance of information security, the level of information security, appropriate to the organization and its individual security responsibilities." This definition emphasizes the need for employees to understand the importance of information protection, the level of security required by the organization, and personal responsibility for maintaining information security.
The first aspect of information security awareness has three key elements – the importance of information security, the level of information security and the individual's security responsibility (Safa et al., 2016). Employees must understand why information protection is important, what measures the organization applies to ensure protection, and what their responsibilities are in that context. This understanding includes the consequences of insufficient information security, including loss of user trust, financial losses and damage to the organization's reputation.

Kruger's definition emphasizes that awareness of information security is not only about passive understanding, but about actively recognizing the importance, applying rules and taking responsibility for protecting information within the organization.

Another aspect of information security awareness focuses on employee engagement and adherence to information security best practices. This aspect is fully consistent with the knowledge-attitude-behavior (KAB) model (Khan et al., 2011), which recognizes that increasing employees' knowledge of information security policies and procedures leads to an improvement in their attitude towards the rules and ultimately, to better behavior in the field of information security.

The HAIS-Q model, as a tool for measuring information security awareness, has a significant contribution in this context. It is used for the information security process by various populations, including students, the general public and employees from various sectors. The HAIS-Q model provides a comprehensive picture of employees' awareness of information security, identifying areas where there is a lack of understanding or application of rules, allowing organizations to target education and training (Papp & Lovaas, 2021), while more detailed focus areas will be described below.

Measuring information security awareness plays a key role in improving information security in organizations. The HAIS-Q model stands out because of its comprehensiveness and proven validity and reliability, organizations can monitor progress, adapt their training and awareness strategies, and respond more effectively to changes in the technological environment and security threats.

Information security awareness consists of understanding the importance and level of information protection, as well as the commitment and behavior of employees in accordance with best practice. The HAIS-Q model represents a key instrument for organizations in achieving a higher level of information security and protecting vital resources from potential threats.

Managing an organization's information security is an extremely complex issue that requires careful planning and implementation of various strategies. One of the key aspects in preserving information security is the human factor. In this context, the HAIS-Q model, developed by Parsons et al., is an important tool for measuring employees' knowledge, attitudes and behaviors related to information security (Parsons et al., 2014). The model consists of seven focus areas, and analyzes individual, organizational and intervention factors.

The HAIS-Q model is based on the idea that a key component of information security is employee awareness (Parsons et al., 2014). Information security awareness refers to the level of understanding and attention an individual pays to security issues.

Parsons et al. (2014) designed a questionnaire consisting of seven key focus areas of information security policy, relevant to both employers and computer users. The first phase of development of the HAIS-Q questionnaire was based on the results of a study of information security in three Australian government organizations, conducted in 2010. This study used a hybrid methodology, combining an

inductive, exploratory approach (Parsons et al., 2010). The authors identified human errors as the main cause of information security violations, stressing that these errors are more often the result of uncertainty and naivety than malicious behavior. This questionnaire aims to assess the level of awareness, attitudes and behavior of employees regarding key aspects of information security. Each of the seven focus areas provides detailed insight into specific aspects of risk and security threats.

Internet usage is a field that deals with understanding the risks and threats that arise from using the Internet. Items imply the process of visitors safe web pages, downloading unverified files and using security tools while surfing the Internet.

In the area of e-mail usage, the focus is on awareness of phishing attacks, where employees must be able to recognize suspicious e-mail messages, links and attachments. Assessments in this area check whether employees send sensitive information via e-mail, use spam protection and handle attachments properly.

Use of social networking sites assesses awareness of privacy and security when using social networking sites. Items assess whether employees share work information on social networks, share sensitive information, and use privacy settings properly.

Password management is a focus area that focuses on strong passwords and proper password management. The ratings check whether employees use unique passwords, change them regularly, and implement multi-factor authentication.

By considering incident reporting, it is assessed whether individuals know how to properly report suspicious or security-threatening situations. The ratings check whether employees report suspicious activity, device loss or theft, and other incidents that could compromise information security.

Information handling is an area that involves understanding how to handle sensitive information. The assessments check whether employees properly handle sensitive information, keep documents secure and use encryption to protect data.

The final focus area, mobile computing, focuses on awareness of the security risks of mobile devices. The assessments check whether employees are properly securing mobile devices, sending sensitive information over Wi-Fi and detecting the possibility of "shoulder surfing" efforts.

The HAIS-Q model provides a structured basis for assessing employee awareness of key aspects of information security. Based on the results, organizations can develop personalized training programs to improve information security and reduce risks related to unwitting users. The model highlights human errors as a common cause of information security breaches, which points to the importance of education to minimize these errors. Through proper application of the HAIS-Q model, organizations can raise the level of awareness and training of employees, thereby strengthening overall information security.

The HAIS-Q model represents a significant advance because it provides empirical support, quantification, contextual analysis, and reliability. It was developed through a rigorous research process that included conceptual development, validity testing, and reliability testing.

The HAIS-Q model consists of 63 items, where the model underwent validity and reliability testing, including test-retest reliability and calculation of Cronbach's alpha coefficient. The results showed high validity and reliability of the HAIS-Q questionnaire.

The importance of awareness of information security among employees is crucial for preserving information security in organizations. Human errors are often the cause of information security breaches, and the HAIS-Q model provides an effective tool for measuring and analyzing human factors in this area. Its strengths, including empirical support, quantification and context analysis, make it a relevant and useful tool for improving security strategies and culture in organizations. The quantitative measurement it provides enables more precise analysis and monitoring of efficiency through training and education programs, thus providing organizations with a practical and efficient tool for managing human factors in the field of information security.

4. Conclusion

Information and communication technology has brought a revolution in the way of doing business, especially through ubiquitous electronic commerce, eliminating time and space barriers, which are characteristic of traditional shopping models. However, this progress is accompanied by a growing number of challenges, especially in the field of information security. Data breaches have become a problem with major consequences for organizations, including high recovery costs, loss of customer trust and reduced sales. A holistic approach to information security, encompassing technical, managerial and human aspects, is becoming imperative for successful business in the digital age.

One of the key challenges is the customer's perception of financial risks, especially in connection with electronic payments. Building customer trust in online transactions is becoming key to business sustainability. Various factors contribute to data theft, including human error, loss of paper documents and insider threats. Therefore, it is imperative that organizations focus their attention on information security policies, employee training, and security awareness.

Human resource management becomes crucial in the context of information security. Information security policies must become an integral part of the organizational culture, and employee training should emphasize the importance of adhering to security procedures. Studies indicate that human factors are often the key cause of safety incidents, which highlights the need for increased employee awareness and education (Parsons et al., 2014).

In order to effectively manage information security, organizations should adopt a holistic approach that integrates technical, managerial and human dimensions. Technical measures, such as data encryption and firewall systems are necessary, but they are not sufficient by themselves. Managerial aspects, including defining security policies, monitoring and responding to incidents, are also essential. However, the key role lies in the human factor, where information security awareness becomes the line of defense against threats.

In this context, the importance of the HAIS-Q model in measuring information security awareness is particularly emphasized. This model provides a structured framework for assessing the human aspects of information security, taking into account different dimensions, such as awareness, education and behavior of employees. The HAIS-Q model enables organizations to identify points of weakness, develop targeted training and implement policies aimed at increasing the level of security awareness.
By incorporating the HAIS-Q model into the information security strategy, organizations can achieve long-term security culture improvement. Measuring security awareness is becoming a key indicator of success, allowing organizations to identify areas that require additional effort and investment. Also, the HAIS-Q model contributes to the creation of a proactive approach to safety, where prevention and education are placed in the foreground, instead of a reactive approach after an incident occurs.

Modern organizations face increasing information security challenges in the digital age. A holistic approach, which includes technical, managerial and human aspects, becomes the key to preserving the integrity of information. Information security awareness, especially measured through the HAIS-Q model, is becoming the cornerstone of effective security management. Organizations that recognize these challenges and take adequate steps towards building a strong security culture will be ready to face increasingly sophisticated threats and maintain the integrity of their information in the digital world.

5. Literature

1. Alavi, R., Islam, S., Jahankhani, H., Al-Nemrat, A. (2013). Analyzing human factors for an effective information security management system. *International Journal of Secure Software Engineering (IJSSE)*, 4(1), 50-47.
2. Da Veiga, A., Astakhova, L., Bitha, A., Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. *Computers and Security*, 92, 101713.
3. Harmon, R. R., Auseklis, N. (2009). *Sustainable IT services: Assessing the impact of green computing practices*. In PICMET'09-2009 Portland International Conference on Management of Engineering & Technology (pp. 1707-1717). IEEE.
4. Khan, B., Alghathbar, K.S., Nabi, S.I., Khan, M.K. (2011). Effectiveness of information security awareness methods based on psyshological theories. *African journal of business management*,

5(26), 10862.
5. Kruger, H., Drevin, L., Steyn, T. (2010). A vocabulary test to assess information security awareness. *Informationa Management and Computer Security*, 18(5), 316-327.
6. Mitchell, G. E. (2014). Strategic responses to resource dependence among transnational NGOs registered in the United States. *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 25, 67-91.
7. Papp, G., Lovaas, P. (2021). Assessing Small Institutions Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q). In *Intelligent Computing: Proceedings of the 2021 Computing Conference*, Volume 3 (pp. 933-948). Springer International Publishing.
8. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. DSTO-TR-2484: Report published by Defence Science and Technology Organisation.
9. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and security*, 41, 165-176.
10. Safa, N.S., Von Solms, R., Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and security*, 56, 70-82.
11. Skopik, F., Settanni, G., Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60, 154-176.
12. Spremić, M., Šimunić, A. (2008). *Cyber security challenges in digital economy*. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346), Hong Kong, China.
13. Snyman, D. P., Kruger, H. (2021). Collective information security behaviour: a technology-driven framework. *Information and Computer Security*, 29(4), 589-603.
14. Zimba, A., Chishimba, M. (2019). Understanding the evolution of ransomware: paradigm shifts in attach structures. International Journal of computer network and information security, 11(1), 26.