Volume: 5, Issue: 1
Page: 55-60
2023

Journal of Scientific Reports

Journal homepage: ijsab.com/jsr

# The Security Issues in The Analysis of Information Management Systems

**Mustafa Sahib Shareef & Mahmood Alkhazaali**

## Abstract

The security issue in the design of information management systems is considered one of the vital issues, in the era of information technology and the information revolution, securing information has become a very necessary requirement. In this paper, the issue of analyzing information management systems was discussed with an emphasis on the security aspect of the analysis process. It is not possible to build and design information management systems without analyzing the full requirements of these systems, including security requirements. The analysis phase is useful to developers in studying and analyzing all system requirements to avoid potential risks, including security risks. It is necessary to try to avoid serious information breaches. If this happens, it is important for the system to have a specific mechanism to detect them and reduce the damage that resulted from them, as well as knowing the reason for their occurrence. Developing a layer of analysis of the security requirements at each stage of the analysis and developing a specific mechanism to detect violations that may occur to the system will be sufficient to increase the reliability of these systems.

**JSR**
Accepted 06 June 2023
Published 12 June 2023
DOI: 10.58970/JSR.1025

ISSN: 2708-7085



**Keywords:** *IMS, Security Issues, Data Security, ISMS.*

About Author (s)

**Mustafa Sahib Shareef** (Corresponding author), Al Muthanna University, Al-Muthanna, Iraq.
**Mahmood Alkhazaali**, Al Muthanna University, Al-Muthanna, Iraq.

## 1. Introduction

Information Management System (IMS) is a software system that helps organizations manage and organize data and information. The global data sphere is expected to reach 175 zettabytes by 2025, emphasizing the need for effective IMS (Kenneth et al., 2017) IMS enables data-driven decision-making, can reduce operational costs by up to 20%, and is a top priority for businesses. IMS can face a range of security threats such as unauthorized access, data breaches, malware attacks, and phishing scams. These attacks can lead to significant consequences for organizations, including data loss, financial loss, legal penalties, reputational damage, and loss of customer trust. Attackers can exploit vulnerabilities in software, hardware, or human behavior to gain access to sensitive information (Ivan et al., 2020)

Cyber threats on IMS are on the rise, with the average cost of a data breach reaching $4.24 million in 2021, according to a report by IBM. The same report found that the average time to identify and contain a data breach was 287 days, highlighting the potential impact of these threats. Additionally, a survey by Accenture found that 68% of business leaders feel their cybersecurity risks are increasing, emphasizing the ongoing importance of effective IMS security measures (Balking, 2019). To address the security threats facing IMS, organizations can take a multi-layered approach that includes analyzing the types of threats they face, existing studies can be leveraged to identify best practices and emerging threats. Employee training and awareness programs can also help reduce the risk of human error leading to security incidents (Brazevich, 2020). The research contribution will be to improve the understanding of cybersecurity threats to IMS and to develop effective strategies to protect against them. The research findings will be of value to organizations seeking to enhance their cybersecurity posture and protect against cyber threats (Yeboah-Boateng, 2018).

## 2-Background

The security of IMS is critical as they store sensitive and confidential information such as financial records, medical records, personal information, and intellectual property (Atoum, 2014). Any breach of security can result in severe consequences such as financial loss, reputational damage, legal liability, and even threats to national security. Hackers, cybercriminals, and other malicious actors are constantly seeking ways to exploit vulnerabilities in IMS and gain unauthorized access to sensitive data (Hughes, 2013). ISMS, or Information Security Management System, is a framework for managing and protecting an organization's sensitive information assets. Cyber Security Standards are a set of guidelines and best practices that help organizations establish effective security controls and processes to protect against cyber threats (Somepalli, 2020). Effective IMS and ISMS are critical components of a strong cybersecurity posture. They enable organizations to manage and protect their sensitive data, and to respond quickly and effectively to security incidents (Andrzejewski, 2020).

### a-Information Management Systems

Information management systems (IMS) play a critical role in helping organizations make data-driven decisions and improve their overall performance (Gupta, 2005). Information management systems (IMS) can be used to manage a wide range of data, including financial information, customer information, and product information, among others. They can also be used to support various business functions, such as sales, marketing, and customer service. In today's digital age, IMS have become an essential tool for businesses of all sizes to effectively manage and utilize the vast amount of data available to them (Gupta, 2005; Watson, 1997). IMS can be implemented in a variety of ways, such as through software applications, databases, and digital platforms. They can be used by individuals, small businesses, and large organizations.

IMS are used to store, process, and analyze data for a wide range of business applications. This data can include customer information, financial transactions, and other sensitive information.

As a result, IMS are a prime target for cybercriminals seeking to steal sensitive data or disrupt business operations (Watson, 1997; Choobineh, 2007). The figure1 shows the elements of the information management system.

**b-Information Security Management System (ISMS)**

An Information Security Management System (ISMS) is a set of policies, procedures, and guidelines that help organizations manage their information security risks, protect their critical data, and ensure the confidentiality, integrity, and availability of their information (Solana-González, 2019). ISMS is based on the principle of continuous improvement, which means that organizations must regularly review and update their information security policies and procedures to adapt to changes in the threat landscape and ensure that they remain effective (Solana-González, 2019; Al-Dhahri, 2017). The implementation of an ISMS is not only important for protecting an organization's information assets but is also a requirement for compliance with various industry standards and regulations. Examples of such standards include ISO 27001, which is an international standard for information security management, and the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements for organizations that handle payment card data (Berisha-Shaqiri, 2014). Overall, an ISMS is a critical component of a strong cybersecurity posture, helping organizations manage risks and protect their operations and reputation (Pedro, 2019).

**c. Cyber Security Standards**

Cybersecurity standards are sets of guidelines, procedures, and practices that help organizations to protect their computer systems, networks, and data from unauthorized access, theft, damage, or other cyber threats. These standards are developed and maintained by industry organizations, government agencies, and other professional bodies to establish a common language and framework for cybersecurity (Morris., 2015).

The cybersecurity standards cover a wide range of topics such as access control, cryptography, network security, application security, incident response, and risk management. Some of the popular cybersecurity standards are (Atoum, 2014):

1. **ISO/IEC** 27001: This standard outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
2. **NIST** Cybersecurity Framework: This framework provides a set of guidelines, standards, and best practices to manage and reduce cybersecurity risks.
3. **PCI DSS:** This standard provides requirements for organizations that handle credit card information to ensure the security of cardholder data.
4. **HIPAA**: This standard outline requirement for protecting and securing personal health information.
5. **GDPR:** This standard provides a set of regulations for data protection and privacy for citizens of the European Union.

Adherence to cybersecurity standards can help organizations to achieve compliance, improve their security posture, and build trust with their customers and stakeholders.

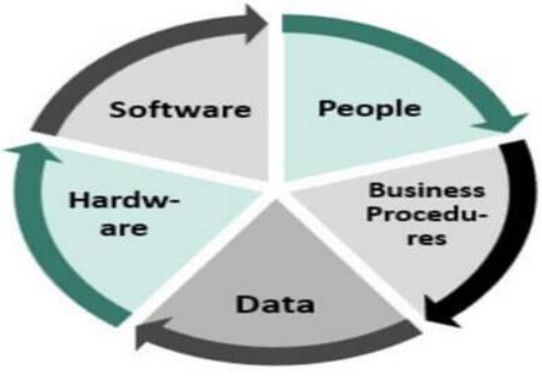


figure1 elements of the information management system IMS

**3-Related works**

Benamar (2019) presented a systematic review of security requirements engineering approaches for information systems. The authors identified and analyzed 42 papers and found that there is a need for more comprehensive and integrated approaches to security requirements engineering.

Hernández Ramos (2018) proposed a framework for identifying and analyzing security requirements in IS. The framework includes four stages: identification, analysis, specification, and validation. The authors applied the framework to a case study and found that it was effective in identifying and analyzing security requirements. Lee (2018) analyzed security issues in cloud-based IS. The authors identify several security threats and vulnerabilities, including data breaches, denial-of-service attacks, and unauthorized access. They also propose several security solutions, such as encryption, access control, and intrusion detection systems. Khajeh-Hosseini (2016) presented a security risk analysis of an IS in a governmental organization. The authors used a risk assessment framework to identify and analyze security risks and proposed several risk mitigation strategies, such as access control, security monitoring, and security testing. Hsu (2015) analyzed security issues in business process management systems (BPMS). The authors identify several security threats and vulnerabilities. They also propose several security solutions, such as access control, encryption, and audit logging. Grefen (2013) described a security analysis of distributed information management systems (DIMS). The authors identify several security threats and vulnerabilities, such as network attacks, data tampering, and denial-of-service attacks. They also propose several security solutions, such as access control, encryption, and intrusion detection systems.

**4-The proposed mechanism**

The proposed mechanism to address Investigating Cybersecurity Threats in Information Management Systems Analysis consists of five steps, see Figure 2, as follows:

1. **Threat Modeling:** This involves identifying the possible threats to the information management system, determining the likelihood of each threat occurring, and prioritizing the most significant threats to address.
2. **Risk Assessment:** This involves evaluating the potential impact of each threat and determining the level of risk associated with each. This step helps to prioritize the most critical security risks to address.
3. **Security Controls:** This involves implementing security controls to prevent, detect, and respond to potential security threats. Examples of security controls include firewalls, access controls, encryption, and intrusion detection systems.
4. **Monitoring and Testing:** This involves continuously monitoring the information management system for potential security threats and vulnerabilities and testing the effectiveness of security controls.
5. **Incident Response:** This involves developing a plan for responding to security incidents, including procedures for containing the incident, investigating the cause, and restoring the system to normal operation. This mechanism could be implemented using a variety of security frameworks and methodologies, such as the NIST Cybersecurity Framework or ISO/IEC 27001, depending on the specific needs and requirements of the information management system being analyzed. Proposed mechanism for Investigating Cybersecurity Threats in Information Management Systems Analysis:

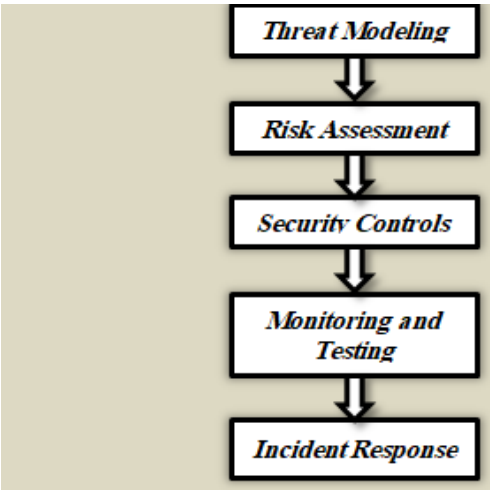


Figure ٢ The general outline of the proposed mechanism

**Input Data:** The proposed mechanism will rely on both primary and secondary sources of data. Primary data will be collected through surveys, interviews, and observations of organizations'information management systems. Secondary data will include relevant literature on cybersecurity threats to information management systems.
**Processing the Data:** The collected data will be processed through various techniques, including statistical analysis, content analysis, and data mining. Statistical analysis will be used to identify trends and patterns in the data, while content analysis will be used to identify common themes and issues related to cybersecurity threats.
**Techniques Used**: The proposed mechanism will use a variety of techniques, including threat modeling, vulnerability assessments, and risk assessments, to analyze the cybersecurity threats facing information management systems. Threat modeling will help identify potential threats and vulnerabilities, while vulnerability assessments will identify weaknesses in the system's security. Risk assessments will help organizations determine the likelihood and potential impact of security incidents.
**Outcome:** The proposed mechanism will help organizations develop a comprehensive understanding of the cybersecurity threats facing their information management systems. The outcome will be a set of actionable recommendations for improving the organization's cybersecurity posture.
**Evaluation Metrics:** The proposed mechanism evaluation metrics will include the effectiveness of the approach in identifying cybersecurity threats, and the impact of the recommendations on the organization's overall cybersecurity posture.

## 7-Discussion

Security issues in the analysis of information management systems are of critical concern, as these systems often contain sensitive and valuable data. There are many different types of security issues that can arise in these systems, including data breaches, unauthorized access, denial-of-service attacks, and malicious code injection. These security threats can come from both external and internal sources, and they can have serious consequences, including financial losses, reputational damage, and legal liabilities. To address these security issues, it is important to have a comprehensive and integrated approach to security. This includes identifying and analyzing security risks, developing and implementing security solutions, and continuously monitoring and updating the security measures in place. This requires collaboration between different stakeholders, including IT professionals, security experts, business managers, and end-users. One of the key challenges in addressing security issues in information management systems is keeping up with the constantly evolving security landscape and stay informed and adapt the security measures in place to address these new risks. This requires ongoing training and education, as well as regular updates to software and hardware systems. Another important consideration in addressing security issues in information management systems is the balance between security and usability. While it is important to have strong security measures in place, these measures should not impede the usability of the system or make it difficult for end-users to access the data they need. Finding the right balance between security and usability requires careful consideration and ongoing evaluation. Overall, addressing security issues in the analysis of information management systems requires a multi-faceted approach that considers the different types of security threats, the evolving security landscape, and the balance between security and usability. By taking a proactive and comprehensive approach to security, organizations can minimize the risks associated with these systems and protect their valuable data.

## 6-Conclusion

In conclusion, investigating cybersecurity threats in information management systems is critical for organizations to protect their sensitive information assets and ensure the continuity of their operations. This paper has highlighted the importance of information security

management systems (ISMS) and cybersecurity standards in managing risks and protecting information assets. The proposed approach for investigating cybersecurity threats in information management systems can help organizations identify potential security breaches, vulnerabilities, and other security incidents, and provide actionable recommendations for improving their cybersecurity posture. By implementing the recommended measures, organizations can better protect their information assets, demonstrate their commitment to protecting sensitive information, and maintain stakeholder trust. Overall, the proposed approach can help organizations stay ahead of cybersecurity threats and ensure the confidentiality, integrity, and availability of their information.

## References


Benamar, A. (2019). A Systematic Review of Security Requirements Engineering Approaches for Information Systems. *In IEEE Transactions on Dependable and Secure Computing,10.1109/TDSC.2018.2803587*, pp. 78-109.

Khajeh-Hosseini, A. D. G. (2016). Security Risk Analysis of Information Systems: A Case Study of a Governmental Organization. *Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2015.2404655.

Al-Dhahri, S. (2017). Information security management system. *International Journal of Computer Applications,10.5120/ijca2017912851.*, 29-33. .

Andrzejewski, K. (2020). ISMS. . *Management Sciences*, 24. 1-9. 10.15611/ms.2019.4.01.

Atoum, I. O. (2014). A holistic cyber security implementation framework. *Information. Management & Computer Security*, 22 (3), 251-264.

Balking, L. (2019). IMS framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy.*

Berisha-Shaqiri, A. (2014). IMS and Decision-Making. *Academic journal of interdisciplinary studies MCSER publishing, Rome-Italy*, v3n2p19.

Brazevich, D. (2020). Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society. *doi: 10.4236/jss.2020.82018.*, pp. 231-241.

Choobineh, J. (2007). Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems.* 958-971.

Grefen, M. H. (2013). Security Analysis of Distributed Information Management Systems. *In International Journal of Network Security*, 12(3), 3.

Gupta, A. &. (2005). IS issues and decisions for small businesses: An empirical examination. Inf. Manag. Comput. Security. 13, 297-310.

Hsu, J. H. (2015). An Analysis of Security Issues in Business Process Management Systems. *In International Journal of Information Security*, 014-0258.

Hughes, J. (2013). Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technology Innovation Management Review*, 3(8).

Ivan, S. & Georgi, T. (2020). Vulnerability and Protection of Business Management System :threats and Challenges. 72, 29-40 .

Hernández Ramos, J. L. (2018). A Framework for the Identification and Analysis of Security Requirements in Information Systems". *In Journal of Information Security*. doi: 10.4236/jis.2018.91004.

Lee, J. Y. (2018). Analysis of Security Issues in Cloud-Based Information Systems. *In IEEE Access*. doi: 10.1109/ACCESS.2820901.

Morris, S. M. (2015). Cybersecurity: Challenges from A Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems*, 16, 191-198.

Pedro, S. (2019). MULTICRITERIA ANALYSIS OF THE COMPLIANCE FOR THE IMPROVEMENT OF INFORMATION SECURITY. *Journal of Information Systems and Technology Management*, 16, 1807-1775.

Solana-González, P. (2019). Multicriteria analysis of the compliance for the improvement of information security. *Journal of Information Systems and Technology Management*, 16. 1-19.

Somepalli, S. (2020). Information Security Management. *HOLISTICA-Journal of Business and Public Administration*, 11. 1-16. .

Watson, R. (1997). Key Issues in IMS: An International Perspective. *J. of Management Information Systems*, 13. 91-116.

Yeboah-Boateng, E. (2018). Cyber-Security Intelligence Gathering: Issues with Knowledge Management. *5225-5634, 10.4018/978*.



**Cite this article:**

**Mustafa Sahib Shareef & Mahmood Alkhazaali** (2023). The Security Issues in The Analysis of Information Management Systems. *Journal of Scientific Reports, 5*(1), 55-60. doi: https://doi.org/10.58970/JSR.1025
Retrieved from http://ijsab.com/wp-content/uploads/1025.pdf

**Published by**