ABEJ

Politechnika Warszawska
Warsaw University of Technology

Applied Business and Economics Journal

e-ISSN: 2956-7432 | 2024 Vol. 2 No 1 pp. 100–124 | DOI: 10.61089/abej.2024.2.87

Technological Advancements and Their Impact on Organisational Information Security

Kozłowski Kajetan[1]

[1] Akademia Sztuki Wojennej (War Studies University)

Recived: 16 April 2024

Accepted: 26 June 2024

Published: 30 September 2024

Abstract:

This paper explores the crucial role of strategic management and integration of information security within organisations to safeguard against diverse threats in a rapidly evolving digital environment. It posits that effective management of information security significantly enhances organisational resilience and protects strategic assets amidst global information exchange and technological advancements. The research employs a systematic literature review method, analysing existing definitions and perspectives on information security, supplemented by an analytical examination of potential vulnerabilities within corporate security systems and a case study of the IBM model in order to provide a comprehensive approach to information security in practice. The study shows that technological progress and the development of comprehensive security frameworks by governmental and non-governmental organisations directly improve the effectiveness of information security measures. Furthermore, it emphasises information as a strategic asset that requires a holistic security approach incorporating organisational and legal measures. The findings advocate for a multidimensional approach to information security, highlighting the necessity of continuous adaptation to effectively combat evolving threats. This comprehensive analysis contributes to the scholarly discourse on information security management, offering insights that can inform future research and practical applications in enhancing organisational resilience.

Keywords:

information security, enterprise security, threat assessment, data protection.

ARTICLE

1. Introduction

In the current information era, the right to access specific data and the capability to utilise it effectively are paramount for regulating not only individual actions but also for shaping a wide range of environments, systems and processes. This elevates data to the status of a strategic asset, a target for expansion efforts, and an object of deliberate destructive actions. Data is a valuable resource that drives and enhances the knowledge base used across various operational spheres of organisations (Białas, 2017).

The profound impact of information on the awareness and competencies of individuals and organisations is undeniable. Data related to specific areas of activity must be protected not only from adversaries, but also from any generally unauthorised disclosure, posing a major challenge for both governmental and non-governmental institutions.

With the universal access to almost all types of information, we face a broad spectrum of potential threats, including the critical risk of unintentional leaks or deliberate acquisition of legally protected data. The issue of information security is perennially relevant and has always accompanied human activity. The intensity of these threats depends on the dynamics of emerging conflicts (Żebrowski, 2013).

Amidst the rapid evolution of technology and the burgeoning global exchange of information, strategic management and integration of information security is paramount for safeguarding organizational assets against a spectrum of threats, both internal and external. This paper delves into this issue as its main hypothesis: the integration and strategic management of information security significantly bolsters an organization's resilience, safeguarding its strategic assets, and is thus of vital operational importance.

To dissect the multifaceted nature of information security further, the article delineates several detailed hypotheses. Firstly, it examines the correlation between technological progress and the efficacy of information security measures. It posits that technological advancements directly enhance the effectiveness of information security protocols, thereby mitigating the risk of unauthorized data breaches and fortifying an organization's security stance.

Secondly, the role of both governmental and non-governmental organizations in shaping the information security landscape is scrutinized. These entities are instrumental in developing

standards and regulations that underpin effective information security frameworks, thereby influencing the adoption of comprehensive security measures across diverse sectors.

Thirdly, the article explores the notion of information as a strategic asset, necessitating a holistic security approach. This approach transcends technological solutions, incorporating organizational and legal measures to combat a wide array of threats.

Lastly, the paper acknowledges the ongoing challenges organizations face in implementing and maintaining robust information security practices. Despite the availability of sophisticated security solutions, evolving threats, regulatory complexities, and the continuous need for employee training and awareness present enduring challenges.

The objective of this article is to explore the various dimensions of information security in contemporary business environments, underscoring the critical importance of a multidimensional approach to protecting data and information assets. Through an examination of current practices, challenges, and strategies in information security management, this paper aims to shed light on enhancing organizational resilience against multifaceted threats to their data assets. By providing a comprehensive analysis, the study seeks to contribute to the scholarly discourse on information security management, offering insights that inform future research and practical applications in the field.

2. Methodology

The methodology of this study was designed to explore the domain of information security and its associated threats within the corporate sector. At the inception, a systematic literature review was conducted, which served as the cornerstone of the research. This method facilitated a comprehensive examination of existing definitions and perspectives on information security, alongside identifying contemporary threats to corporate information systems.

Through meticulous analysis of scholarly works, both from Polish and international authors, the study was able to collate and synthesise a wide array of definitions pertaining to the core concepts under investigation. This synthesis not only yielded a collective representation of these definitions but also enabled the distillation of key elements inherent in the discussed terms. Subsequently, these elements formed the foundation for developing original definitions of information security and information safety.

Furthermore, the study employed an analytical approach to pinpoint potential vulnerabilities within enterprise information security systems, highlighting areas susceptible to cyber threats. This methodological framework thus provided a structured pathway to explain the intricacies of information security, offering a novel contribution to the academic discourse by integrating and refining the conceptual understanding of information safety and security threats in a business context.

To enhance the robustness of the research, the author incorporated the empirical method of a case study of IBM's comprehensive approach to information security, which shows a real-world application of integrated security strategies in a large, multinational corporation.

The author acknowledges the limitations inherent in the adopted methodology but hopes it will pave the way for further research in this area to fully elucidate the threats to corporate information security. This nuanced approach aims to contribute to the scholarly discourse by offering a refined understanding of information security challenges, underscoring the importance of continual exploration and adaptation in the face of evolving digital threats.

2.1 Security of information and information security

The right to access data and the capability to utilise it are fundamentally crucial for shaping both individual and collective actions (Maśloch, 2018). Consequently, information is regarded as a strategic asset requiring special protection against potential threats, both external and internal. In the era of global data exchange, where technological advancement offers unprecedented communication and information processing capabilities, new security challenges are emerging. These challenges not only underscore the importance of data protection but also indicate the need for continuous adaptation of security strategies to changing conditions.

Threats to data security are diverse and evolve with technological progress, necessitating integrated actions by both governmental and non-governmental organisations to protect information. These actions should encompass legal, organisational, and technical arenas to effectively safeguard information resources from unauthorised access, leaks, or destruction.

Selected approaches to information security, which will serve as a reference point for further considerations on the comprehensive process of information protection in modern organisations, are presented in Table 1.

Table 1

Sample definitions of the term Security of Information

Author	Definition
Liderman, 2017, p. 13.	• Information security means justified (e.g., by risk analysis and adopted risk management methods) confidence that losses will not be incurred due to undesirable changes resulting from the realisation of threats to essential values of information quality criteria
Denning, 2002, p. 41.	• Defensive actions conducted within the realm of informational warfare aimed at protecting information resources against the following attacks: increasing accessibility for the attacking party, reducing accessibility for the defending party, or reducing integrity
Pawłowski et al., 2020, p. 23-24.	• Protection of information against unauthorised: access, illegal use, disclosure, disruption, modification, recording, and destruction. This is ensured through physical, electromagnetic, and transmission protection, as well as cryptography and preventing access to devices and networks
Białas, 2017, p. 27-28.	• The field concerned with protecting data regardless of the form in which it is stored, processed, or transmitted. This includes ensuring the confidentiality, integrity, and availability of information, in both teleinformatics systems and analogue formats such as paper documents or microfilms, as well as in the context of information exchanged between individuals. Information security, therefore, requires a holistic approach that considers all potential vectors of attack and threats to data, regardless of their form
Ciborowski, 2001, p. 186.	• Information security is "information defence", which involves preventing and hindering the acquisition of data about the physical nature of the current and planned state of affairs and phenomena within one's own operating space, as well as hindering the introduction of informational entropy into messages and physical destruction to data carriers
Ministerstwo Cyfryzacji [Polish Ministry of Digitization], 2023, p. 17.	• Protection of information and systems from unauthorised access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability. Careful implementation of information security measures is key to protecting an organisation's information assets, as well as its reputation, legal position, staff, and other material and immaterial assets
Microsoft Corporation, 2024, n/p.	• A set of security tools and procedures that broadly protect a company's confidential information from abuse, unauthorised access,

Author	Definition
	disruptions, or destruction. InfoSec includes physical and environmental security, access control, and cybersecurity
Polski Komitet Normalizacyjny, PKN, [Polish Committee for Standardization], 2018, n/p	• Information security means protecting information from various threats in such a way as to ensure continuity of operations, minimise losses, maximise return on investments, and business-related activities

Source: author's own elaboration.

The summary of the presented definitions of information security extracts common elements that can be considered key to understanding this concept. Primarily, information security is characterised as a multidisciplinary field focused on protecting data, regardless of the form in which it is stored, processed, or transmitted.

The analysis of issues related to information security takes on special significance in the context of continuous changes and evolution driven by rapid progress in technology, including methods of accumulation, storage, processing, and distribution of data. From an informational aspect, security protection is associated with safeguarding the strategic interests of organisations against both deliberate and accidental actions that may be directed against their informational resources. Therefore, activities related to ensuring information security should be conducted within comprehensive strategies aimed at protecting organisations from any potentially negative impacts in the fied of information (Stanik & Kiedrowicz, 2018).

Selected approaches to information security, which will serve as reference points for further consideration of the holistic process of information protection in modern organisations, are presented in Table 2.

Table 2

Example definitions of the term 'information security'

Author	Definition
Pawłowski et al., 2020, p. 24.	• A type of security concerning information at all stages of its production, processing, storage, and transmission. Implemented through countering unlawful access and any interference with data, information, and information systems
Stanik & Kiedrowicz, 2018, p. 332.	• Comprises a set of actions, methods, and procedures undertaken by authorised entities aiming to ensure the integrity of collected, stored,

Author	Definition
	and processed information assets, by protecting them against unwanted, unauthorised disclosure, modification, or destruction
Bączek, 2015, p. 71.	• Understood as a state free from threats of information transmission to unauthorised entities, espionage, subversive or sabotage activities • Any action, system, or method aimed at securing information assets that are collected, processed, transmitted, and stored in computer memories and telecommunication networks
Łuczak, 2004, p. 80.	• A component of physical, legal, personal-organisational, and teleinformatic security of an organisation
Werner & Szczepaniuk, 2016, p. 170.	• A state in which the elements of the security system are capable of protecting against current and future disruptions or loss of specific values. Achieved and maintained at a predetermined level of confidentiality, integrity, and availability as well as reliability and integrity of services. Authenticity and accountability of entities are ensured. Users of information and services as well as recipients of information and services are aware and not susceptible to information security threats. Threat actors have limited opportunities to exploit teleinformatic systems to generate threats
Potejko, 2009, p. 194.	• A collection of actions, methods, and procedures undertaken by authorised entities, aiming to ensure the integrity of collected, stored, and processed information assets, by protecting them against unwanted, unauthorised disclosure, modification, or destruction
Żebrowski & Kwiatkowski, 2006, p. 452.	• Ensuring by a given entity the integrity, completeness, and reliability of possessed information assets in every form, not just electronic. Thus, it refers to all kinds of efforts aimed at protecting held information, crucial in the context of security (thus affecting the smooth functioning of state structures and society), as well as securing informational advantage by acquiring new or more up-to-date data and disinformation actions against potential adversaries

Source: author's own elaboration.

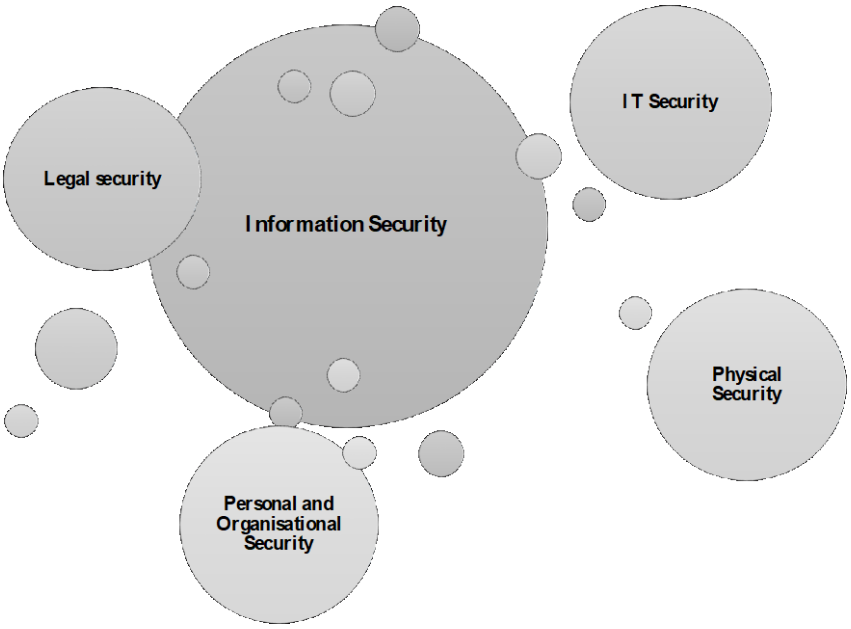
Comparing the presented definitions of the term "information security," several key common aspects can be observed across all descriptions. Primarily, information security is portrayed as a comprehensive action that covers all stages of the information lifecycle: from its creation, through processing and storage, to transmission. The central goal of these actions is protection against unauthorised access, disclosure, modification, destruction, and other forms of interference in data, information, and information systems.

2.2 Information threats

Security is an unceasing process in which efforts are made to refine methods that ensure a sense of protection. The perception of and approach to security as a priority area of interest for firms is manifested in their responses to potential threats (Żywiołek, 2020). These actions, although demanding and often associated with high costs, are crucial. However, the challenges they present may compel some organisations to abstain from their implementation. The fundamental elements of information protection are illustrated in Figure 1.

Figure 1

Components of information security



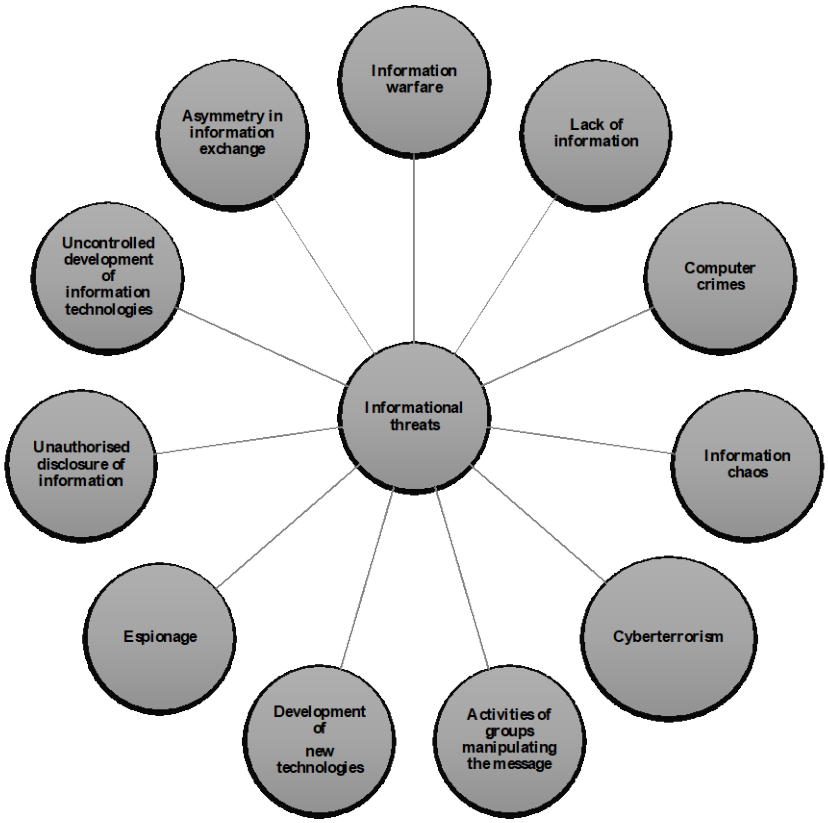
Source: Zarządzanie bezpieczeństwem informacji (p. 80), J. Łuczak,, 2004, Wydawnictwo „Oficyna Współczesna".

The categorisation of dangers to data security and their precise definition forms the foundation of information protection within a company. In the field of political science, particularly those definitions concerning security, threats are often classified as challenges. Proper identification and response to such challenges can convert them into opportunities, while challenges that are improperly recognised or identified too late may evolve into threats. This approach to threats is also reflected in other academic disciplines, such as management and sociology. Organisations focused on innovation and the pursuit of new solutions encounter new challenges and threats

daily, with their spectrum constantly expanding. Figure 2 illustrates selected threats to the information security of the organisation.

Figure 2

Categories of information threats

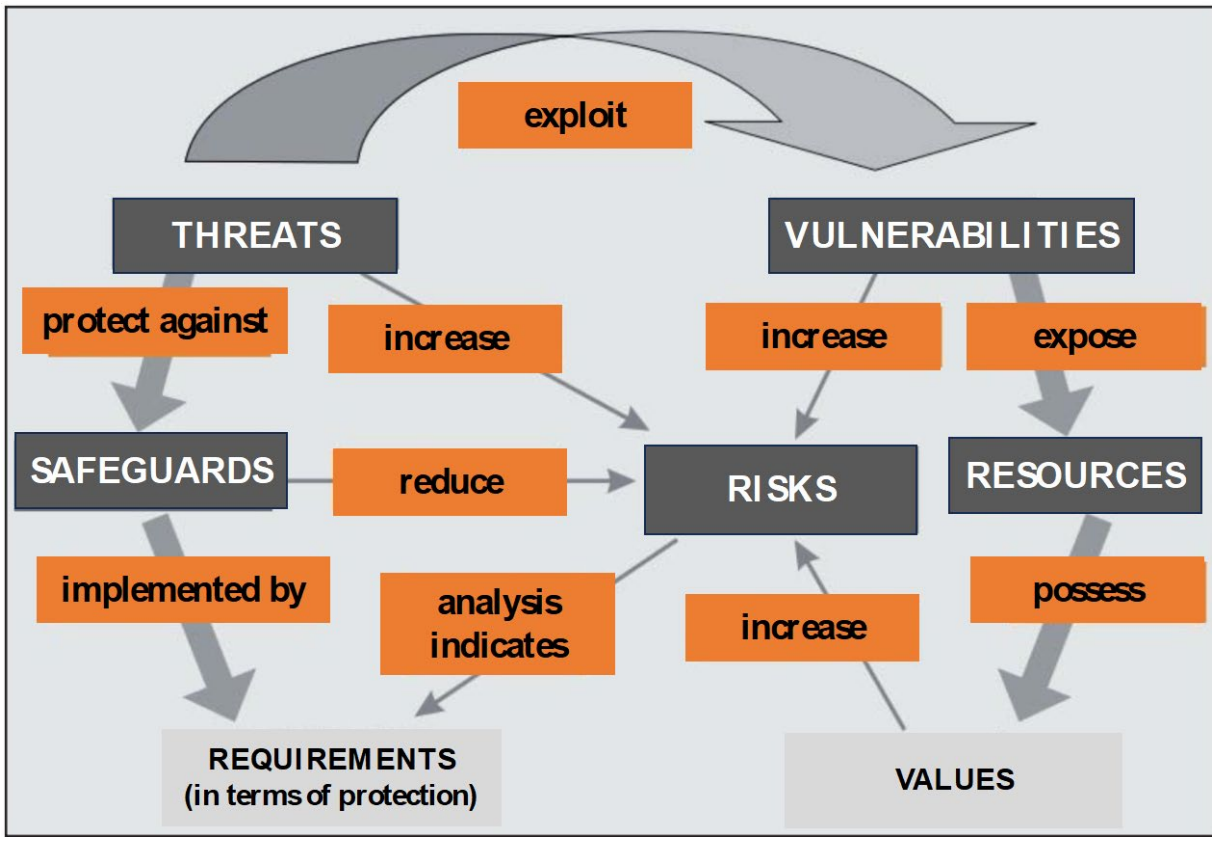


Source: Zagrożenia informacyjne a bezpieczeństwo państwa polskiego (p. 30), P. Bączek, P, 2015, Wydawnictwo Adam Marszałek.

Engaging in commercial activities is associated with risk, which manifests in the organisation as specific dangers. The diversity of these risks is broad and may evolve over time. The elements of security and their interrelationships are depicted in Figure 3.

Figure 3

Security Elements and Their Interrelations

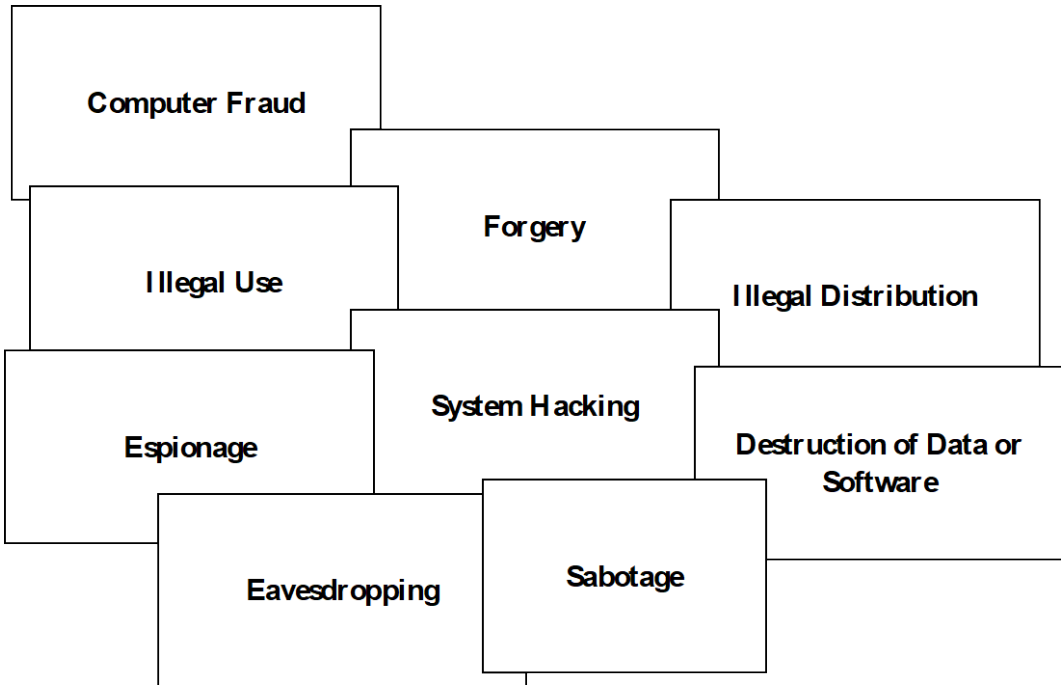


Source: Bezpieczeństwo informacyjne organizacji (p. 170), J. Werner, & E. Szczepaniuk, 2016, Zeszyty Naukowe AON, 4(105).

Łuczak (2006), in his deliberations on uncertainty and risk within the context of the global information society, points out the necessity to associate risk with the concept of threats, particularly with the accumulation of risks arising from various sources of danger. The level of uncertainty is influenced by dynamic technological development. Experts note that advancements in information technology create conducive conditions for criminal activity. On one hand, new technologies facilitate decision-making at various management levels within a company; on the other hand, they introduce new types of threats (Żebrowski & Kwiatkowski, 2006). These dangers may pose risks to the human, material, financial, and informational assets of an organisation (Żywiołek, 2020). Figure 4 illustrates typical forms of criminal activity in the IT sector and their interrelationships, as considered by Fischer (2000) in the early 21st century, outlining nine key categories for information security within an organisation.

Figure 4

Categories and Relationships of Computer Crimes



Source: Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne (p. 33), B. Fischer, 2000, Wydawnictwo Zakamycze.

Organisations are faced with the task of securing the confidentiality, integrity, and availability of operations associated with the collection, processing, and distribution of information, so that access is limited to employees authorised based on their professional role or assigned duties. Five main areas of risk for IT infrastructure are distinguished, encompassing (Fischer, 2000, p. 33):

a) the skills and trust of employees,
b) management of systems and networks,
c) telecommunications infrastructure,
d) creation of hardware and software,
e) policies for the use of information systems,
f) handling of data carriers.

In the face of numerous risks associated with information security, it is crucial to identify the most critical areas of potential threats in order to then design and implement strategies for their protection, restrict access for authorised users, organise training, and conduct continuous monitoring. An increase in the scale of economic crime and other irregularities is observed in enterprises (Żywiołek, 2020). Table 3 presents types of threats to the business sector, including economic crimes, cybercrime, and espionage activities.

Table 3

Types of Threats to the Business Sector

Crimes in Enterprises		
Economic and Banking	**Computer**	**Human Activity**
• Forgery of public documents • Forgery of business documents • Fraud	• Destruction of information • Data forgery • Eavesdropping • Sabotage • Piracy • Vandalism • Hacking • Cracking	• Technological intelligence • Commercial intelligence • Competitive intelligence

Source: *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa* (p. 267), R. Borowiecki and M. Kwieciński (Eds.), 2003, Wydawnictwo Zakamycze.

Criminal incidents in the business sphere belong to a distinctive category, as they pose a risk not only to the companies or institutions themselves but also to their assets. This pertains to data accumulated in information databases, financial resources, as well as the intangible values of the enterprise, such as reputation, established relationships, or commercial entitlements (Borowiecki & Kwieciński, 2003).

Informational threats to organizations can be classified according to the origins of their sources as follows (Żebrowski & Kwiatkowski, 2006, p. 72):

a) Internal – generated within the organization itself, encompassing the risk of data loss or destruction, or the inability to process data due to random events or errors, as well as the risk arising from the actions of individuals acting dishonestly within the company

b) External – arising from actions outside the company's structure, including the risk of data loss, destruction, or the prevention of their processing through deliberate or unintended actions by third parties against systems or networks
c) Physical – where the loss, destruction of data or the inability to process it are the result of failures, disasters, or other unexpected events that impact the IT infrastructure or network devices

One of the key sources of data security risk in companies is unauthorized access to protected information by persons who have access to it. Applying regulations on the protection of confidential data also presents challenges. Advances in ICT and market globalization favor the automation of business and accounting processes, facilitate global communication, and enable transactions with partners from different parts of the world without the need for direct contact (Żywiołek, 2020). However, the benefits of digitizing business activities are associated with risks. IT systems, which are designed to collect, process, and share information quickly, can attract the attention of individuals with criminal intentions. The diversity and nature of these systems, particularly their origins, spark interest not only among intelligence agencies and other official institutions potentially posing a threat but also among terrorist groups and individuals. These systems are vulnerable to actions by anyone who possesses the necessary knowledge and skills (Żywiołek, 2020).

Data security breaches, on data that is classified as confidential or protected for state or corporate reasons, aim to gain control over secured information systems. Such incidents of computer security occur when actions are deliberately targeted at violating the integrity of systems. Two main categories of attacks can be distinguished (Barczyk & Sydoruk, 2003, p. 70):

a) Active attacks, which involve direct or indirect interventions in the system, altering data flow or introducing false information
b) Passive attacks, characterized by a lack of direct impact on the system, including the interception of communication or network monitoring to identify key components, such as servers or workstations

The risk of an attack significantly increases when there is a likelihood of (Barczyk & Sydoruk, 2003, p. 68):

a) unauthorized access to confidential or official data stored, processed, or transmitted – without impacting the system
b) unauthorized actions affecting the system, which can result in changes in network functioning, access to data, the introduction of false information, damage to data and system resources, or unauthorized changes to information

In an era of unlimited access to information and abundant online resources, internet users must be aware of the risks posed by unauthorized individuals. During attempts to breach a system, the intruder follows a set pattern, identifies system weaknesses, and gains access to its resources. After gaining control of the system, they undertake actions aimed at erasing evidence of their presence. Threats can take various forms, but the consequences are always the same – data loss or destruction, resulting in damage to the organization (Żywiołek, 2020).

The identification of threats enables the initiation of risk assessment within an organisation. Effective risk management is crucial for creating a comprehensive information security plan. Risk analysis in the realm of data security allows for the determination of the total risk, which should be reduced to a level deemed acceptable. Elements that can contribute to the emergence of threats to information security include the following (Ciecińska et al., 2006, p. 171):

a) distribution of resources over a vast area
b) use of computer equipment without licenses
c) use of unauthorized software
d) use of equipment and software of unknown origin
e) resistance from users and developers against the implementation of information security measures

In the field of information security, distinguishing between passive and active attacks is crucial for understanding and minimising potential threats to organisational data and systems. Passive attacks, characterised by unauthorised access attempts without system interference, aim to covertly gather data, posing a significant risk to confidentiality. On the other hand, active attacks involve direct interaction with the system, potentially altering data or system functionality, compromising the integrity and availability of information. Both types of attacks require robust security measures and continual vigilance to protect the digital assets of a business.

In response to data security challenges, enterprises have undertaken initiatives to implement and optimise their data protection procedures. These activities have included the development of (Stanik & Kiedrowicz, 2018, p. 335):

a) Security management systems within the organisation
b) Security strategies
c) Data protection policies
d) Information security management systems
e) Numerous guidelines, standards, and technologies related to data protection

The diversity and complexity of these methods have led companies to explore alternative approaches and unified data protection strategies. Considering that information threats can arise from various situations, such as shortages, access limitations, excess, manipulation, forgery, illegibility, illegal acquisition, and obsolescence of information, these threats are characterised as situations with restrictions or abuses in lawful access to current, credible, integral, and confidentially protected information (Stanik & Kiedrowicz, 2018). In summary, for effectively maintaining a high level of information security, organisations should implement as many measures internally as possible, based on proven security management models and best practices in formulating security policies, or delegate these responsibilities to experts in information security.

A key function in directing information processes within a company, reflecting its main goals, is maintaining data security. The priority of information management is to ensure that all operations and managerial functions at every organisational level are integrally linked with information processes. Given the critical role that information security and information management play in business operations, the implementation of these strategies is viewed as necessary and appropriate. The issues addressed form the foundation for creating a model of the system and managing information security in the enterprise.

3 Results

The cited definitions emphasise ensuring three fundamental objectives of security of information: confidentiality, integrity, and availability of information. The key elements of these definitions can be encapsulated as follows:

a) Trust in protection against threats – highlighting the importance of justified trust in systems and procedures aimed at protecting against undesirable changes and the realisation of threats that could negatively impact the essential values for the quality of information
b) Defence against attacks – defensive actions intended to protect informational resources from attacks that can reduce the availability, integrity, or confidentiality of data, are a common denominator in the definitions, underscoring the necessity of active defence against potential threats
c) Holism in information protection – the need for a holistic approach to information security, which includes physical, electromagnetic, and cryptographic aspects, as well as protection against unauthorised access to devices and networks. This approach is essential to address all potential vectors of attack
d) Protection against unauthorised actions – emphasis on protection against unauthorised access, exploitation, disclosure, disruption, modification, registration, and destruction of information, which is crucial for maintaining data security
e) Protection irrespective of data form – a significant element is the emphasis that information security concerns the protection of data regardless of its form
f) Complexity of security tools and procedures – highlighting the role of a set of security tools and procedures in protecting information from abuses and unauthorised access, which includes physical, environmental security, access control, and cybersecurity

A common element in these definitions is viewing security of information as a key component of an organisation's strategy, aimed not only at data protection but also at ensuring operational continuity, minimising losses, and maximising the return on investment. Security of information is thus understood as a comprehensive activity that requires engagement at various organisational levels and the application of diverse methods and protection tools.

The themes of integrity, confidentiality, and availability of information resources emerge clearly as key values that information security aims to protect. Furthermore, information security is perceived not only in the context of protection against external threats, such as espionage or subversive activities, but also in terms of ensuring the reliability and integrity of services and the authenticity and accountability of entities.

Besides technical and operational aspects, the definitions also highlight an organisational and legal dimension, emphasising the role of procedures, methods, and actions taken by authorised

entities to protect information. The awareness of users and recipients of information about potential threats and their ability to counter these threats is also deemed important.

Based on the above analysis, the following definition of the term 'information security' can be proposed: an integrated system of actions, methods, procedures, and technical, organisational, and legal measures aimed at protecting information at all stages of its lifecycle – from generation through storage, processing, to transmission. Its fundamental goals are to ensure the confidentiality, integrity, and availability of information resources, protect against all forms of unauthorised interference, including access, disclosure, modification, destruction, or espionage.

This also includes maintaining the reliability and integrity of services, ensuring the authenticity and accountability of entities operating within the system, and promoting awareness and resilience to threats among users and recipients of information. As a result, information security supports the continuity of an organisation's operations, protecting its information resources against current and future threats, contributing to the maintenance of its stability, reputation, and informational advantage.

4 Discussion

The study presents compelling evidence supporting the hypothesis that strategic management and integration of information security significantly enhance organizational resilience. The results, reflecting the systematic literature review and analytical approach taken in the methodology, confirm that information security measures directly correlate with the ability of organizations to mitigate risks associated with unauthorized data breaches and other security threats.

The findings of this study are significant as they validate the increasing dependence of organizations on sophisticated information security strategies in the face of growing cyber threats. The implications of these findings are broad, impacting policy makers, IT managers, and organizational leaders by emphasizing the need for comprehensive and integrated security measures. These results not only underscore the importance of technological advancements in security protocols but also highlight the critical role of regulatory frameworks established by both governmental and non-governmental organizations.

The results align well with previous studies that have emphasized the importance of a holistic approach to information security. For instance, research by Białas (2017) and Żebrowski (2013) has also highlighted the strategic value of information as an asset and the necessity of protecting it through integrated organizational, legal, and technological measures. This study further enriches the academic discourse by providing empirical evidence that supports these theoretical assertions.

The findings advocate for a multidimensional approach to information security, which includes not only technological solutions but also organizational and legal strategies. This approach is crucial for addressing the diverse threats that organizations face in the digital age such as polymorphic malware, zero-day exploits and social engineering (Paul, 2024). A notable example of this approach can be seen in IBM's information security strategy (IBM Corporation). IBM, a global leader in technology and consulting services, faces significant security challenges due to its vast and complex IT infrastructure. To mitigate these risks, IBM implemented a comprehensive security framework that integrates advanced threat detection technologies, such as AI and machine learning, with strategic management practices (IBM Corporation2).

IBM's adoption of a Zero Trust security model, combined with continuous employee training and collaboration with external partners, has significantly enhanced its resilience to cyber threats. The company's proactive approach to regulatory compliance further ensures the protection of sensitive data across its global operations. As a result, IBM achieved a 50% reduction in security incidents within the first year of implementing these measures (IBM Corporation3). IBM's comprehensive approach to information security, which integrates advanced technological solutions with strategic management practices, serves as a valuable model for other organizations. By adopting a multi-layered security framework, IBM has effectively protected its digital assets and maintained compliance with international regulations, illustrating the importance of a holistic and proactive approach to information security management. This case study underscores the effectiveness of a holistic and integrated approach to information security, demonstrating how strategic management and technological advancements can work together to protect organizational assets against a wide array of threats.

The study’s emphasis on the importance of strategic management in information security adds a valuable layer to our understanding of how information security can be woven into the fabric of organizational strategy, rather than being viewed as merely a technical or reactive measure.

One of the key takeaways from the study is the necessity for continuous improvement and adaptation in information security practices. The dynamic nature of cyber threats requires that organizations not only implement current best practices but also continuously evaluate and adapt their security strategies to anticipate and mitigate future risks (Obi et al., 2024). This aspect is crucial for maintaining not just security but also competitive advantage in an increasingly digital marketplace.

Drawing on conclusions from recent academic work, including studies by Pachghare (2019) and presentations of findings at the 30th USENIX Security Symposium by Nicolas Huaman and others (Huaman et al., 2021), it is evident that understanding the nature of information security threats and implementing comprehensive security frameworks is highly desirable, indeed essential. These studies highlight the importance of adopting multi-layered security strategies that address various attack vectors and ensure the resilience of information systems against both types of threats. By combining technical measures, policy formulation, and staff training, organisations can significantly reduce their vulnerability to these pervasive security challenges.

Based on the findings, future research could explore the specific impacts of various technological advancements on the effectiveness of information security measures. Additionally, more empirical studies could be conducted to determine the most effective combinations of organizational, legal, and technological strategies for different types of organizations in various sectors.

In conclusion, this discussion integrates the study's findings with existing research, offering a comprehensive analysis of the strategic management of information security. It highlights the necessity for a proactive, integrated approach to protecting information assets, which is essential for enhancing organizational resilience and maintaining operational continuity in the face of evolving security threats (Obi et al., 2024).

5 Conclusion

This paper provides a comprehensive analysis of information security, affirming its significance as a strategic asset essential for both individual actions and broader environmental interactions. The discussion revolves around the premise that strategic management and integration of information security are crucial for protecting organisational assets against various threats.

The paper posits that technological advancements significantly enhance information security measures, thereby reducing the risk of unauthorized data breaches and strengthening the security stance of organizations. It further discusses the pivotal role of governmental and non-governmental organizations in forming the landscape of information security through the development of standards and regulations.

Information is emphasized as a strategic asset that necessitates a holistic security approach, extending beyond technological solutions to include organisational and legal measures aimed at combating a broad spectrum of threats. Despite the existence of advanced security solutions, challenges such as evolving threats, regulatory complexities, and the ongoing need for employee training pose significant obstacles to implementing robust information security practices.

This comprehensive approach combining a systematic literature review and case study methodology provides a robust framework for understanding and improving information security in organizations. The findings from IBM's case study offer valuable insights into practical applications of advanced security measures and strategic management, contributing significantly to the scholarly discourse on information security management.

The paper recognizes the dynamic nature of threats to data security, which evolve with technological progress and necessitate integrated responses from various sectors to effectively safeguard information resources. The study underscores the necessity of continuous adaptation of security strategies to address these evolving threats and protect information against unauthorized access, leaks, or destruction.

In conclusion, the paper emphasizes the critical importance of a multidimensional approach to protecting information assets and enhancing organizational resilience against multifaceted threats. This comprehensive analysis contributes significantly to the scholarly discourse on information security management, providing insights that inform future research directions and practical applications in the field.

6 Suggestions

After analysing the conducted research and based on an analysis of trends in the field of management and quality sciences, the author proposes the following suggestions for the area under study:

1. **Emerging Technologies**: Explore the integration of AI and machine learning to enhance predictive capabilities in information security
2. **Cross-Sectoral Standards**: Evaluate the effectiveness of current security standards across various sectors and develop unified frameworks
3. **Human Factors**: Investigate the impact of organizational culture and user behavior on the effectiveness of security protocols
4. **Cybersecurity Resilience Metrics**: Develop and validate metrics to assess the resilience of information systems
5. **Legal and Ethical Considerations**: Study the balance between enhancing security measures and maintaining privacy rights

These suggestions aim to drive forward the scholarly discourse in information security, focusing on technological, organisational, and strategic aspects that can enhance the understanding and implementation of effective security measures.

References

Bączek, P. (2015). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego [Information Threats and the Security of the Polish State]*. Wydawnictwo Adam Marszałek.

Barczyk, A., & Sydoruk, T. (2003). *Bezpieczeństwo systemów informatycznych zarządzania [Management Information Systems Security]*. Dom Wydawniczy Bellona.

Białas, A. (2017). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie [Information and Services Security in Modern Institutions and Companies]*. Wydawnictwo Naukowe PWN.

Borowiecki, R., & Kwieciński, M. (Eds.). (2003). *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa [Environmental Monitoring, Information Flow and Security: Towards Enterprise Integrity]*. Wydawnictwo Zakamycze.

Ciborowski, L. (2001). *Walka informacyjna [Information Warfare]*. Wydawnictwo Adam Marszałek.

Ciecińska, B., Łunarski, J., Perłowski, R., & Stadnicka, D. (2006). *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie [Enterprise Security Management Systems]*, Oficyna Wydawnicza Politechniki Rzeszowskiej.

Denning, D. E. (2002). *Wojna informacyjna i bezpieczeństwo informacji [Information Warfare and Information Security]*. Wydawnictwo WNT.

Fischer, B. (2000). *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne [Computer Crimes and Information Protection: Legal and Criminological Aspects]*. Wydawnictwo Zakamycze.

Huaman, N., Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). *A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises*. 30th USENIX Security Symposium. Retrieved February 22, 2024, from https://www.usenix.org/system/files/sec21-huaman.pdf

IBM Corporation (No date). *IBM Security*. Retrieved June 24, 2024 from https://www.ibm.com/security

IBM Corporation2 (No date). *Securing a global solutions landscape*. Retrieved June 24, 2024 from https://www.ibm.com/case-studies/sutherland.

IBM Corporation3 (No date). *Simplifying secure identity and access for over 27 million users*. Retrieved June 24, 2024 from https://www.ibm.com/case-studies/ibm-on-ibm-security-verify

Liderman, K. (2017). *Bezpieczeństwo informacyjne. Nowe wyzwania [Information Security: New Challenges]*. Wydawnictwo PWN.

Łuczak, M. J. (Ed.). (2004). *Zarządzanie bezpieczeństwem informacji [Information Security Management]*. Wydawnictwo „Oficyna Współczesna".

Łuczak, M. J. (2006). *Społeczeństwo informacyjne jako społeczeństwo ryzyka [The Information Society as a Risk Society]*. In W. Haber & M. Niezgoda (Eds.), *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne [The Information Society: Functional and Dysfunctional Aspects],* 400-409 Wydawnictwo Uniwersytetu Jagiellońskiego.

Maśloch, P. (2018). *Globalizacja a zarządzanie bezpieczeństwem współczesnych organizacji [Globalisation and Security Management of Contemporary Organisations]*. Wydawnictwo ASzWoj.

Microsoft Corporation. (2024). *Co to jest bezpieczeństwo informacji (InfoSec)? [What is Information Security (InfoSec)?]* Retrieved February 15, 2024, from https://www.microsoft.com/pl-pl/security/business/security-101/what-is-information-security-infosec.

Ministerstwo Cyfryzacji. (2023). *Bezpieczeństwo informacji – wprowadzenie. Narodowy standard cyberbezpieczeństwa NSC 800-12 [Information Security – An Introduction. National Cybersecurity Standard NSC 800-12]*.

Obi, O., Akagha, O., Dawodu, S. Anyanwu, A., Onwusinkwue, S., & Ahmad, I. (2024). Comprehensive Review on Cybersecurity: Modern Threats and Advanced Defense Strategies. *Computer Science & IT Research Journal, 5*(2), 293-310. Doi: https://doi.org/10.51594/csitrj.v5i2.758

Pachghare, V. K. (2019). *Cryptography and information security (3rd ed.)*. PHI Learning Pvt. Ltd.

Paul, A. L. (2024). *The Role of Artificial Intelligence in Enhancing Data Security*. Retrieved June 24, 2024 from https://www.researchgate.net/publication/381004546_The_Role_of_Artificial_Intelligence_in_Enhancing_Data_Security

Pawłowski J., Zdrodowski B., & Kuliczkowski M. (2020). *Słownik terminów z zakresu bezpieczeństwa [Dictionary of Security Terms]*. Wydawnictwo Adam Marszałek.

Polski Komitet Normalizacyjny. (2018). *Zarządzanie Bezpieczeństwem Informacji [Information Security Management]*. Retrieved February 15, 2024, from https://www.pkn.pl/informacje/2018/01/zarzadzanie-bezpieczenstwem-informacji

Potejko, P. (2009). *Bezpieczeństwo informacyjne [Information Security]*. In K. A. Wojtaszczyk & A. Materska-Sosnowska (Eds.), *Bezpieczeństwo państwa: wybrane problemy [State Security: Selected Issues,]* (pp. 193-212). Oficyna Wydawnicza Aspra.

Stanik, J., & Kiedrowicz, M. (2018). Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacyjnego [The Model of an Organisation's Security Management System as the Basis for Forming Information Security Policy]. *Ekonomiczne Problemy Usług, 2*(131), 331-346, DOI: 10.18276/EPU.2018.131/1

Werner, J., & Szczepaniuk, E. (2016). Bezpieczeństwo informacyjne organizacji [Organisational Information Security]. *Zeszyty Naukowe AON, 4*(105), 167-187.

Żebrowski, A. (2013). Bezpieczeństwo informacyjne Polski a walka informacyjna [Information Security of Poland and Information Warfare]. *Roczniki Kolegium Analiz Ekonomicznych, 29*, 447-463.

Żebrowski, A., & Kwiatkowski, M. (2006). *Bezpieczeństwo informacji III Rzeczypospolitej [Information Security of the Third Polish Republic]*. Oficyna Wydawnicza Abrys.

Żywiołek, J. (2020). *Zarządzanie zasobami informacji i wiedzy jako determinanta bezpieczeństwa przedsiębiorstwa [Managing Information and Knowledge Resources as a Determinant of Enterprise Security]*. Wydawnictwo Politechniki Częstochowskiej.