INFORMATION SECURITY CHALLENGES IN THE USE OF DIGITAL TOOLS FOR DATA PROCESSING AND MANAGEMENT

UDC: 004.056:[005.334+005.53]
DOI: https://doi.org/10.53486/tids2025.30

CEBAN SVETLANA
ASEM, Chisinau, MD 2005, Republic of Moldova
ceban.svetlana@ase.md
ORCID ID: 0009-0006-5957-7666

Abstract. The accelerated pace of digitalization has fundamentally transformed the way information is collected, processed, and used. This process brings significant benefits but also major vulnerabilities in the field of information security. Digital technologies – ranging from common applications and online platforms to cloud-based solutions – have become indispensable for the efficiency of educational, economic, and administrative activities. However, the increasing reliance on technology exposes organizations to increasingly complex cyber threats.

This article examines the main information security risks associated with the use of digital tools in data processing and management, drawing on theoretical approaches as well as recent practical examples. Three major categories of challenges are highlighted: technical (ransomware, phishing, software vulnerabilities, and dependence on cloud infrastructures), legal and regulatory (arising from GDPR, NIS2, and other European frameworks), and organizational and human (limited resources and the human factor as the weakest link).

The conclusions emphasize that information security is not solely a technological issue but requires an integrated approach, combining advanced technical solutions with effective organizational policies and legal compliance. Practices such as data encryption, multi-factor authentication, continuous user training, and the principle of "privacy by design" are essential for strengthening organizational resilience against present and future digital threats.

Keywords: information security, cyber threats, ransomware, phishing, cloud computing, organizational resilience.

JEL Classification: M15, O33.

INTRODUCTION

Digital transformations over the past decade have fundamentally changed the way companies, educational institutions, and organizations manage data. Modern technologies – from office software applications and online collaboration platforms to cloud services – have become essential for economic, administrative, and educational processes. These tools provide clear benefits in terms of efficiency, accessibility, and cost optimization, but at the same time they increase exposure to cyber threats and information security risks.

Alongside the benefits of digitalization, related challenges have also intensified: increasingly sophisticated cyberattacks, data breaches, and difficulties in meeting information protection requirements. Threats such as ransomware [1], phishing [1], software vulnerabilities [5], and growing dependence on cloud infrastructures [1] significantly affect both the academic and corporate sectors. In addition, strict compliance obligations under European regulations (GDPR [2], NIS2 [3]) further increase the overall level of complexity.

In this context, the present article analyzes the most significant information security challenges associated with the use of digital tools for data processing and management. It also discusses practical solutions and recommendations, emphasizing an integrated approach that combines technical, organizational, and legal dimensions to strengthen the resilience of institutions and companies against current and emerging digital threats.

INFORMATION SECURITY CHALLENGES

The transformations of today's digital environment generate a wide variety of risks that directly impact information security. These risks are not uniform but fall into several categories, depending on their nature and their effects on organizations. First, there are technical challenges, linked to cyberattacks and IT infrastructure vulnerabilities. Second, there are legal and regulatory challenges, related to compliance with strict data protection and cybersecurity requirements. Finally, organizational and human challenges must also be considered, arising from user behavior, limited resources, and an organizational culture that does not sufficiently prioritize security. Examining these three dimensions is essential for understanding the complexity of information security and for identifying solutions suited to the current context.

A. Technical Challenges

1. **Ransomware Attacks.** Ransomware is among the most widespread and dangerous forms of cyber threats [1]. Such attacks encrypt data and demand payment to restore access. Universities and companies are often targeted because their activities rely heavily on uninterrupted access to digital platforms and critical databases. Several European academic institutions have had to suspend online operations temporarily due to ransomware, disrupting education and damaging their reputation [1]. The consequences extend beyond financial losses, affecting institutional credibility and partner trust.

2. **Phishing and Social Engineering.** Unlike purely technical attacks, phishing exploits human errors such as negligence and lack of vigilance. Attackers use convincing messages to obtain sensitive data (passwords, access codes) or trick users into installing harmful software. In both academic and corporate settings, this can result in compromised email accounts, internal systems, and confidential files. The absence of regular staff training and excessive trust in seemingly safe sources make phishing a persistent cause of security breaches [1].

3. **Software Vulnerabilities.** Everyday applications – from text editors and spreadsheets to collaborative platforms and database systems – may contain hidden vulnerabilities. Failing to apply updates or using software from unreliable sources opens the door for attackers. Zero-day exploits can fully compromise IT infrastructures. Outdated, unpatched systems make institutions particularly vulnerable [5].

4. **Dependence on Cloud.** The extensive use of cloud services (Google Workspace, Microsoft 365, AWS, Dropbox) has reshaped how data is stored and shared. However, increased dependence on cloud providers brings additional risks: misconfigured sharing settings, account compromises, and legal issues related to cross-border data storage. These risks can only be reduced through strict access control and constant monitoring [1].

B. Legal and Regulatory Challenges

1. **GDPR Compliance.** The GDPR requires organizations to follow strict rules for handling personal data [2]. In practice, this is difficult, especially when data is transferred to servers outside the EU (such as Google Workspace or Microsoft 365). Many institutions lack resources for full

compliance, such as appointing a Data Protection Officer (DPO) or conducting regular audits. The threat of large fines – up to EUR 20 million or 4% of global turnover [GDPR, art. 83] – increases pressure on organizations [2].

2. **NIS2 Directive and Cybersecurity.** Adopted in 2022, NIS2 strengthens cybersecurity rules across the EU [3]. It expands to cover educational institutions, digital providers, and strategic companies. Requirements include reporting incidents within 24 hours, conducting assessments, and applying strict risk management measures. For many organizations, especially those with limited budgets, meeting these obligations requires significant investments in IT systems and specialized staff.

3. **Unregulated Emerging Technologies.** The fast development of new digital technologies creates legal and security challenges. In the absence of clear rules, responsibility for data breaches or flawed decisions remains uncertain, shifting between developers, service providers, and end users. The lack of proper regulation may also reduce transparency and fairness in critical sectors such as education, healthcare, and employment. The EU has begun drafting new frameworks, but until their full application, a regulatory gap persists [4].

C. Organizational and Human Challenges

1. The Human Factor. End users remain the weakest link in information security. Studies show that most successful cyber incidents arise more from human mistakes than technical flaws. Weak passwords, shared credentials, and careless handling of suspicious emails create major risks. In educational settings, with many users on the same platforms, the danger is even greater. Without regular training and awareness, the human factor remains a critical vulnerability (IBM Cyber Security Report, 2023) [7].

2. Limited Financial Resources. Many organizations, especially in education and the public sector, lack adequate budgets for cybersecurity [1]. This leads to reliance on outdated systems, missing updates, weak backup solutions, and a shortage of specialized staff. Such conditions make them attractive targets for advanced attacks (OECD Report on Cybersecurity, 2022).

3. Organizational Culture. In many institutions, information security is still treated as an administrative formality rather than a strategic priority [6]. The absence of clear policies and accountability results in rules being applied superficially, lowering overall protection. By contrast, organizations that view security as an investment in stability and credibility succeed in reducing their exposure to risks [6].

STATISTICAL ANALYSIS

To better understand the depth and complexity of information security risks faced by organizations, it is important to examine the evolution of ransomware attacks between 2022 and 2024. Data provided by international cybersecurity bodies, such as ENISA [1] and the Microsoft Digital Defense Reports [5], show a steady and significant rise in the number of incidents.

This upward trend reflects not only the growth of criminal activity in the digital sphere but also the ongoing weaknesses of IT infrastructures – including the lack of regular updates, configuration mistakes, and insufficient user training.

As shown in Table 1, the number of ransomware attacks increased sharply over the three-year period, with a growth rate of +26% in 2023 and +15.5% in 2024 compared to previous years.

Table 1. Evolution of Reported Ransomware Attacks Worldwide (2022–2024).

Year	Estimated Number of Reported Attacks (millions)	Annual Growth Rate (%)
2022	493	-
2023	623	+26%
2024	720	+15,5%

Furthermore, Figure 1 shows the global evolution of reported ransomware attacks, emphasizing both their continuous growth and the magnitude of the phenomenon.

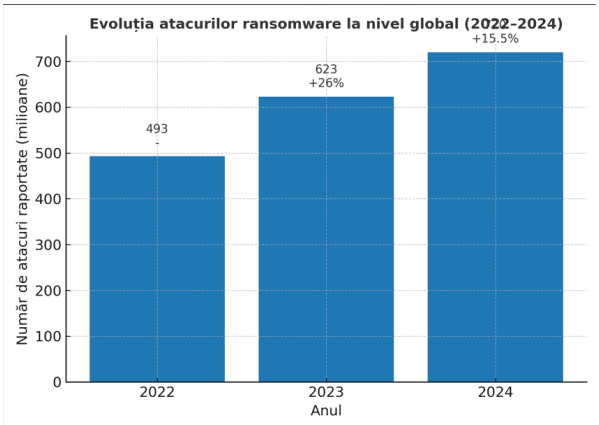

Figure 1. Evolution of Ransomware Attacks Worldwide, 2022–2024.

CASE STUDIES OF RANSOMWARE INCIDENTS

To better illustrate the figures presented in Table 1 and Figure 1, several real cases of ransomware attacks are worth mentioning.

In **December 2019**, *Maastricht University* in the Netherlands was hit by the Clop ransomware. Attackers encrypted Windows servers, including backup systems, and the university had to temporarily shut down many of its online services. The incident caused major disruption to teaching and administration, and restoration took several weeks [8].

In **March 2023**, the *Hospital Clínic de Barcelona* in Spain suffered a ransomware attack that paralyzed its IT infrastructure. Emergency rooms, laboratories, and pharmacy systems were severely affected, and thousands of medical appointments had to be canceled due to the inability to access digital records [9].

Another significant case occurred in **Andalusia, Spain**, where a ransomware attack targeted the regional health service. Internal documents and patient data were leaked, while many healthcare services were temporarily disrupted. According to ENISA, about 82% of affected medical entities reported delays in patient care as a direct consequence of the incident [10].

These examples confirm that ransomware attacks are not abstract threats but concrete realities affecting universities, hospitals, and public institutions. The impact extends beyond financial losses, directly influencing essential services, user trust, and institutional reputation.

The analysis of real incidents highlights not only the vulnerabilities of digital infrastructures but also the urgent need for proactive measures. These experiences show that effective protection requires more than reaction; it demands preventive strategies tailored to organizational realities.

SECURITY STRATEGIES AND RECOMMENDATIONS

Studying information security challenges represents only the first step in understanding the complexity of today's digital environment. To effectively counter these risks, organizations need to design and apply integrated solutions that reduce vulnerabilities and strengthen resilience. A purely technological perspective is not sufficient, since information security is by its nature multidimensional.

Therefore, a comprehensive strategy is required, combining:

- **technical measures** aimed at protecting infrastructures and data;
- **organizational measures** that engage users and promote a strong culture of security;
- **legal and compliance measures** to ensure conformity with regulations and international standards.

Only through a unified vision, adapted to the specific context of each organization, can a high level of protection against current and future digital threats be achieved.

1. **Technical Solutions.** The first line of defense is the technological component, directly focused on safeguarding systems and sensitive data. Key measures include:
   - **Data encryption** – both in transit and at rest – using strong modern standards (e.g., AES-256, TLS 1.3) to ensure confidentiality even in case of breaches.
   - **Multi-factor authentication (MFA),** which strengthens account protection by combining passwords with biometric factors or one-time codes, significantly reducing the risk of compromise.
   - **Regular application of updates and patches,** essential to eliminate vulnerabilities and prevent zero-day exploitation. Enabling automatic updates is considered best practice.
   - **Periodic backups** in offline environments or secure cloud storage, together with testing recovery procedures, to enable fast restoration after incidents such as ransomware attacks.
   - **Intrusion detection and monitoring** through IDS/IPS solutions and SIEM platforms, ensuring early detection of suspicious activity and preventing large-scale breaches.
2. **Organizational Solutions.** The second level of defense addresses human and institutional factors. No matter how advanced technology is, security remains fragile if users lack training or if internal policies are poorly defined. Essential measures include:
   - **Clear security policies,** specifying access rules, user responsibilities, and applying the "least privilege" principle (minimum necessary access).
   - **Continuous staff training,** with workshops, awareness campaigns, and guidelines to reduce exposure to phishing and social engineering.
   - **Simulations and regular testing,** such as phishing drills or incident response exercises, to measure preparedness in real scenarios.
   - **Business continuity and disaster recovery plans (BCP/DRP),** with concrete procedures for resuming operations after major incidents.
   - **Dedicated roles and resources,** including appointing a Chief Information Security Officer (CISO) or a Data Protection Officer (DPO), even in smaller organizations.

3. **Legal and Compliance Solutions.** A third essential dimension of information security is compliance with existing laws and standards. Beyond technology and organizational aspects, legal adherence is vital both for protecting data and for avoiding penalties. Important measures include:
   - **Applying GDPR principles** [2], such as "privacy by design" and "privacy by default," ensuring data protection from the earliest stages of system and application development.
   - **Meeting NIS2 Directive requirements** [3], which oblige organizations in key sectors to adopt risk management policies, report incidents within 24 hours, and perform regular security audits.
   - **Preparing for new European frameworks,** by reviewing the use of emerging digital tools and aligning internal procedures so that decisions remain transparent and accountable.
   - **Conducting internal and external compliance audits,** to detect vulnerabilities early and implement corrective actions that minimize risks of exploitation.

FINDINGS

The analysis highlights several key aspects related to information security in the context of using digital tools:

• **The evolution of ransomware attacks** confirms a steady increase during 2022–2024, showing that this type of threat continues to be one of the most critical vulnerabilities for modern organizations. The consequences extend beyond financial losses to include operational disruptions, restricted access to essential resources, and reputational damage to affected institutions.

• **The human factor** remains the weakest link in the security chain. Weak passwords, carelessness toward suspicious messages, and insufficient knowledge of security practices directly facilitate the success of cyberattacks. The absence of continuous training and the lack of a security-oriented culture within organizations amplify these risks.

• **Educational institutions** are among the most exposed, due to limited budgets and the large number of users sharing the same platforms. This makes them highly vulnerable to phishing, social engineering, and ransomware attacks, with significant effects on both teaching and administrative processes.

• **Compliance with European regulations** – such as GDPR [2] and NIS2 [3] – represents an additional burden for organizations. Adapting to these requirements requires substantial investment in IT infrastructure, regular audits, and specialized staff, along with constant alignment to an evolving legislative environment.

• **Information security** should not be viewed solely as a set of technical measures but as a multidimensional process. It integrates technological, legal, and organizational components, underlining the importance of a comprehensive and collaborative strategy to reduce risks and strengthen resilience.

The findings summarized above confirm that information security is a challenge that goes beyond technology. They emphasize the importance of integrating technical solutions with legal frameworks and organizational culture, setting the stage for the conclusions drawn in this study.

CONCLUSIONS

The analysis carried out in this article has shown that, in the context of using digital tools for data management and processing, information security is a complex and multidimensional issue. The main risks identified fall into three major categories: technical risks, resulting from cyberattacks and IT infrastructure vulnerabilities; legal and regulatory risks, linked to the requirements of the European framework and the lack of clear standards for new technologies; and organizational and human risks, where limited resources and user-related factors play a critical role.

The conclusions underline that these challenges cannot be solved in isolation but require an integrated strategy that brings together advanced technological measures, effective organizational policies, and legal compliance [1–7]. Practices such as data encryption, multi-factor authentication, regular user training, and the application of "privacy by design" principles show that information security extends beyond the technological domain, also involving managerial, educational, and legal dimensions.

Looking forward, strengthening organizational resilience against digital threats will depend not only on implementing current best practices but also on the ability to adapt continuously to new risks driven by technological innovation and the growing use of cloud services. Only a proactive and holistic approach can transform information security from a source of vulnerability into a factor of stability and credibility for modern organizations.

In the future, the effectiveness of information security will also depend on the capacity of organizations to collaborate at both national and international levels. Sharing knowledge, best practices, and incident reports can significantly improve preparedness against large-scale attacks. At the same time, investments in digital education and awareness programs are essential, ensuring that users at every level, from students to managers, understand their role in protecting data. Strengthening cooperation between institutions, governments, and the private sector can transform information security from a reactive response into a proactive shield, able to support long-term stability and trust in the digital environment.

REFERENCES

1. ENISA. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
2. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 (NIS2 Directive)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
4. European Commission. (2021). *Proposal for Regulation on Emerging Digital Technologies*. COM (2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
5. Microsoft. (2023). *Microsoft Digital Defense Report 2023*. Microsoft Corporation. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
6. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
7. IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach
8. GEANT (2020). *Case Study: What Maastricht University Learned from the Ransomware Attack*. GEANT. https://security.geant.org/case-study-what-maastricht-university-um-learned-from-the-ransomware-attack-part-2/
9. AP News (2023). *Ransomware attack on Barcelona hospital cancels thousands of appointments*. https://apnews.com/article/37e0fee33798c56459e63866ca8b449f
10. ENISA (2023). *ENISA Threat Landscape for the Health Sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf