Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.68

DIGITAL INNOVATION AND CYBER RISKS: A REAL CHALLENGE FOR BUSINESSES IN THE REPUBLIC OF MOLDOVA

TURCAN AURELIA
TIMI, Academy of Economic Studies
Republic of Moldova
e-mail: turcan.aurelia.4u8h@ase.md
ORCID ID: 0009-0003-2512-2231

Abstract:Digital transformation has become a determining factor in competitiveness and sustainable business development at the global level. In the Republic of Moldova, digital innovation manifests itself in the form of the introduction of modern technologies such as cloud solutions, artificial intelligence, e-commerce, and fintech services, which open up significant opportunities for economic growth and expansion into international markets. However, alongside these advantages, the business environment is exposed to an increasingly complex range of cyber risks, from ransomware and phishing attacks to financial fraud and massive data leaks.
The purpose of this study is to analyze the impact of digital innovation on the business environment in the Republic of Moldova and the cyber risks associated with the digital transformation process. The research topic concerns how companies integrate modern technologies (cloud computing, e-commerce, fintech, artificial intelligence) and their degree of exposure to cyber threats. The methodology used consists of an analysis of specialized literature, the national and European regulatory framework, as well as reports on cybersecurity in the business environment.
The results of the study show that enterprises in the Republic of Moldova face serious challenges in ensuring digital security (lack of specialists, inadequate infrastructure, low awareness, incomplete regulations), which leads to vulnerability to cyber-attacks that result in financial losses and damage to reputation.
The findings highlight the need to strengthen the culture of cybersecurity, invest in innovative protection solutions, and promote cooperation between the public and private sectors to reduce vulnerabilities.
Keywords: innovation, cyber risks, information security, digital transformation, business Republic of Moldova.
JEL Classification: O32, O33, M15, K24.

1. Introduction

The modern economy is undergoing a significant digitalization phase, radically changing traditional business models, value chains, and consumer interactions. For the Republic of Moldova, which strives for economic integration with the EU and strengthening its position in the global economy, digital transformation is not only a trend but also a matter of strategic necessity. According to the Digital Economy and Society Index (DESI) 2023, Moldova is advancing in digitalization, moving up four positions compared to 2022 (Digital Economy and Society Index,2023).

Technological innovations in fintech products, e-commerce platforms, cloud computing, and elements of artificial intelligence allow local businesses to optimize processes, enter new markets, and become more competitive.

However, this technological revolution also has a downside. The sudden transition to a digital world significantly expands the attack surface. Moldova is among the top 10 EMEA (Europe, the Middle East, and Africa) countries for attacks on Internet of Things (IoT) devices in 2023, according to a Kaspersky Lab report (Cyber Threat Statistics in the EMEA Region, 2023), indicating a high vulnerability of its digital infrastructure.

The rapid shift to digitalization during the pandemic has led to an explosive increase in cyber incidents—in 2020, their number increased by 45%, with an average annual increase of nearly 140 cyber incidents.

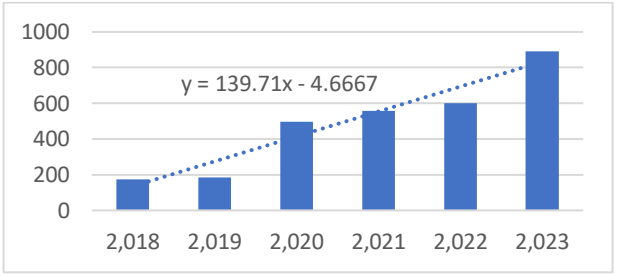


Figure 1. Trend in cyber incidents in Moldova for 2018-2023.
Source: elaborated by the author

Cybercriminals are using increasingly sophisticated methods, and Moldovan businesses, with limited resources and experience, are vulnerable prey. Financial losses, damage to business reputation, and data leaks are just some of the consequences of a successful cyberattack.

Therefore, the relevance of this study stems from the need to consider the dual impact of digital innovation on Moldovan businesses: on the one hand, as an engine of growth, and on the other, as a source of new and complex risks. The purpose of this study is to comprehensively examine this paradox and propose possible ways to minimize cyber risks to ensure sustainable growth for Moldovan businesses.

2. Cybersecurity Situation in the Republic of Moldova

In 2023, the National Cybersecurity Center reported 152 million cyberattacks, and 42% of small and medium-sized enterprises in Moldova suffered from phishing attacks (Report of Digital Transformation Strategy 2023-2030). The paradox of digital transformation in modern Moldova is that the active introduction of technological innovations — from the mass transition to cloud services to the explosive growth of e-commerce — is accompanied by the emergence of fundamentally new and increasingly sophisticated cyber threats.

However, along with these benefits for the business world, an increasingly sophisticated spectrum of cyberthreats is emerging. The Republic of Moldova is gradually making progress in the field of cybersecurity, especially considering its limited resources (GDP per capita is USD 5,700) (World Bank,2024). Let's take a closer look at the case of the Republic of Moldova and its progress in cybersecurity.

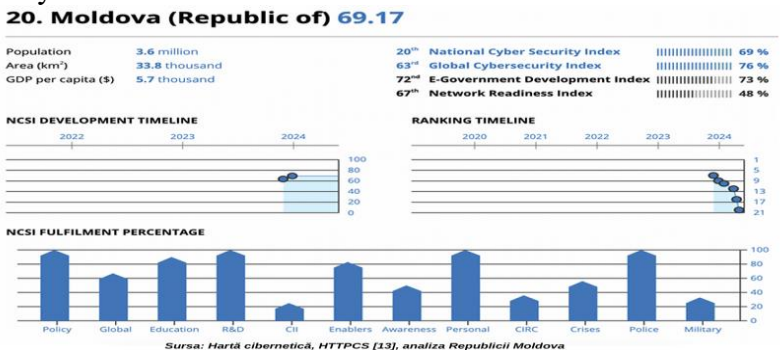


Fig. 2. Moldova's position in international cybersecurity rankings and fulfilment of NCSI indicators.
Source: (PISA,2024)

Let us take a closer look at the situation in the Republic of Moldova and its progress in the field of cybersecurity. Taking into account the data presented in Fig. 2. The following achievements and strengths should be noted positively:

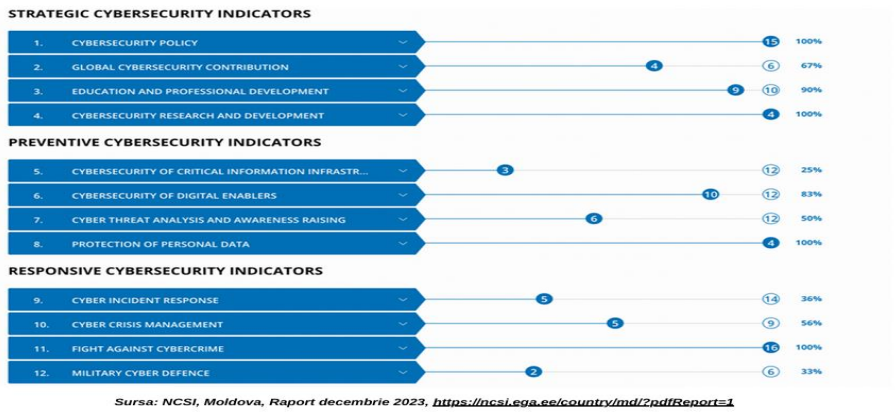
1. Steady improvement in positions in global rankings (PISA,2024)
- o National Cybersecurity Index (NCSI): 69.17% (69th place)
- o Global Cybersecurity Index: 76% (63rd place)
- o E-Government Development Index: 73% (72nd place)

2. Dynamic development in recent years (NCSI Report RM, 2023)
- o According to the NCSI development schedule, a significant improvement in indicators is observed between 2022 and 2024
- o Moldova moved up in the global ranking from 21st to 20th place

3. High level of implementation of strategic indicators (Legea Nr. 48, NCSI Report RM, 2023, Armas Reismary , Taherdoost Hamed,2025)
- o Moldova demonstrates 100% implementation of key strategic objectives
- o A national cybersecurity strategy has been developed
- o Active participation in global cooperation
- o Development of educational programs and advancement of scientific research

At the same time, At the same time, it is necessary to highlight areas for improvement. These include (Network Readiness Index, 2023):

1. **Network Readiness Index**
   - o The lowest score of all the indices – only 48%
   - o Therefore, it is necessary to invest in ICT infrastructure.
2. **Uneven development of different areas**
   - o Strategic indicators achieved 100%
   - o Some operational areas require more attention



Sursa: NCSI, Moldova, Raport decembrie 2023, https://ncsi.ega.ee/country/md/?pdfReport=1

Fig. 3. Detailed assessment of Moldova's cyber resilience
Source: (PISA,2024)

Specific proposals for future growth (Armas Reismary , Taherdoost Hamed,2025)**:**

1. Infrastructure development

a. Increase investment in modernizing network infrastructure.

b. Build systems to protect critical information infrastructure.

2. Human capital development

a. Expand cybersecurity training programs

b. Encourage research and development in cybersecurity.

3. International cooperation

a. Actively participate in international efforts to ensure cybersecurity.

b. Adopt international best practices and standards.

3. The current cyberthreat situation for Moldovan companies

Statistics show an increase in the number of cyberattacks on Moldovan enterprises (Raport-Strategie, 2024):

1. **Ransomware:** Orange Moldova reports that in 2023, the number of ransomware attacks on enterprises increased by 85%. The average ransom amount ranged from €10,000 to €50,000.
2. **Phishing attacks:** These account for 91% of all cyberattacks. In 2023, a 45% increase was recorded compared to the previous year. According to the NCC report, 42% of Moldovan SMEs fell victim to phishing attacks in 2023. The success rate of such attacks was 18% for companies that did not implement email security systems. More than 1,000 phishing attempts against companies are registered monthly.
3. **DDoS attacks:** The number of attacks has increased significantly, with 250 attacks recorded in the first quarter of 2023 alone. The typical attack duration is 3–5 hours.
4. **APT attacks:** The number of sophisticated targeted attacks on key infrastructure is growing.
5. **Social engineering fraud:** In officially disclosed cases alone, BEC (business email compromise) attacks caused financial losses of over 25 million lei in 2023.
6. **Data leaks:** The number of reported data leaks increased by 60% in 2023, with 75% of all reported leaks occurring in the services and retail sectors.

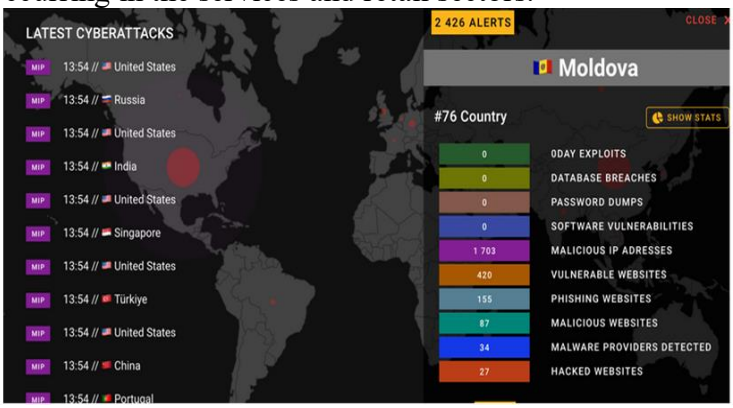


Figure 4. Operational situation: statistics and typology of cyber threats for the Republic of Moldova

Source: (HTTPCS Moldova,2024)

Moldova ranks 76th in the global cyber threat index. According to the presented image, three significant categories of such threats in Moldova should be distinguished (HTTPCS Moldova,2024):

1. **Critical threats:** Zero-day exploits, database breaches, password dumps
2. **Technical vulnerabilities:** Software vulnerabilities, malicious IP addresses, vulnerable websites.
3. **Web threats:** Phishing sites, malicious web resources, hacked websites, malware distributors.

Sursa: Bitdenender [5], Amenințări cibernetice, Hartă în timp real

Figure 5. Cyber activity monitoring: Moldova in a global context

Source: (HTTPCS Moldova,2024)

As a peer adversary, Moldova has a large number of threats (2,426 incidents) and a wide range of attack vectors, from phishing to zero-day exploits. Special attention should be paid to the international nature of threats (from the **USA** (main source), **Russia, India, Singapore, Turkey, Portugal** and **China**), which requires the immediate deployment of comprehensive protection, especially against web threats and data leaks. (HTTPCS Moldova,2024).

These indicators confirm the need to strengthen cybersecurity at both the company and national levels in Moldova.

4. Business Vulnerabilities in Moldova

Statistics show that every year, between 40% and 66% of small and medium-sized enterprises are attacked, with 43% of attacks directly targeting small businesses, which are considered the 'weak link' in the economic chain. (Orange Moldova, 2025)

The consequences of a successful cyberinteraction against a Moldovan company are multifaceted and typically catastrophic:

1. Economic Damage: The direct damage to a typical company from an attack range from 150.000 to 300.000 lei. Taking into account indirect losses (downtime, loss of customers), this amount can reach 1 million lei (Raport-Strategie, 2024).

2. Operational Losses: The average downtime after a ransomware attack is 3-5 business days. 25% of companies attacked are unable to recover all their data even after paying the ransom (Orange Moldova,2025).

3. Loss of reputation: According to a survey, 65% of customers are willing to switch service providers after their data has been compromised (Scoreboard 2023).

4. Legal risks: Since the GDPR came into force, Moldovan companies operating in the EU have reported 12 cases of fines totaling €850,000 (Rusweb, 2023). Research has identified systemic cybersecurity issues:

- Staff shortages: A survey by the Association of ICT Companies confirms a shortage of around 1,200 cybersecurity specialists. 65% of companies struggle to attract talented security professionals (Forbes,2025).
- Budget constraints: Only 15% of SMEs invest more than 5% of their IT budget in security, while international best practice is 10–15% .
- Low awareness: According to an NCC survey, only 38% of Moldovan company employees learned about cybersecurity in the last year (Raport-Strategie, 2024).
- Outdated hardware: 45% of companies still use Windows 7 and previous versions of the OS, which are no longer supported by the manufacturer (Rusweb, 2023).
- Ineffective implementation of the regulatory framework: 32% of companies covered by the Cybersecurity Law fully implement its provisions.

The consequences of a successful cyberattack on a Moldovan company are multifaceted and often catastrophic. Direct financial losses associated with system restoration and ransom payments, operational losses due to business interruptions, irreparable reputational damage, and growing legal risks, all pose a complex challenge to the viability of the enterprise. It is worth noting that most local companies, including SMEs, are technically and financially unprepared for such incidents. The increased intensity and complexity of attacks remind us that cybersecurity is no longer simply a technological issue, but a strategic matter of business risk management.

In this context, effective government regulation capable of creating a unified, secure digital environment is becoming a decisive factor in stability. The state is becoming an important player in creating a secure digital environment, particularly in harmonizing legislation with European standards. Moldova has already taken several important steps in this direction:

- **Europeanization of legislation** (NIS Directive, GDPR) (Rusweb, 2023).
- **Law on Cybersecurity** Nr. 48 din 16-03-2023 (Legea Nr. 48)
- **Establishment of the National Cybersecurity Center:** coordinating responses to cyber incidents, monitoring threats

The EU has provided Moldova with €15 million to improve cybersecurity under the EU4Digital program to address digital security issues and bridge the technology gap (EU4Digital Summit 2023).

Despite this success, strategic development of cyber resilience requires further concerted efforts. Key recommendations are macroeconomic (public policy) and microeconomic (for individual companies):

Recommendations for the government:

1. Create a cybersecurity reward system – tax incentives for businesses implementing secure innovations: provide tax incentives to SMEs investing in cybersecurity (the maximum tax incentive is up to 30% of cybersecurity investments for SMEs), increase the cybersecurity budget (in 2024, the budget will increase by 40% compared to 2023, reaching 85 million lei).

2. Strengthen educational infrastructure – increase the number of state-funded cybersecurity positions: increase the number of state-funded cybersecurity positions to 100 per year. Develop educational programs (to train 240 specialists in 2023, but this is only 20% of current demand).

3. Information Sharing Center: create a national ISAC (Information Sharing and Analysis Center) for businesses.

4. Audit Subsidies: subsidize 50% of the cost of independent cybersecurity audits for small and medium-sized businesses.

5. Expand international cooperation – collaborate with ENISA and NATO (gaining access to key resources and expertise), and learn from Romania's experience, which is particularly valuable for Moldova. Create a "digital bridge" between countries (joint exercises and training of CERT teams, threat intelligence coordination, joint educational programs, and unification of cybersecurity standards).

Recommendations for businesses:

1. Invest in core security practices – use multi-factor authentication and regularly back up data: using multi-factor authentication (MFA) reduces the likelihood of unauthorized access by 99%. Regular data backups allow you to recover data in 95% of ransomware attacks without having to pay the ransom.

2. Refocus security on innovation – security strategies focused on cloud-based structures, API connections, and open innovation.

3. Integrate security into innovation cycles – use the "security by design" principle when developing new digital products and services.

4. Developing cybersecurity competencies – regularly training employees on current cyber threats: companies that regularly train their employees face a 70% reduction in successful phishing attacks.

5. Creating a threat monitoring system – establishing a National Information Sharing Center (ISAC).

6. Creating a Security Operations Center (SOC): companies with a SOC detect incidents on average within 2 hours, compared to 14 days previously.

7. Cyber insurance risk: the cyber insurance market in Moldova grew by 200% in 2023, indicating increased threat perception.

Only in this way can a unified strategy combining government planning and enterprise security ensure the secure growth of Moldova's digital economy in the face of growing cyber threats.

To address digital security issues and bridge the technological divide, Moldova has received €15 million from the EU to strengthen cybersecurity as part of the "EU4Digital" program (EU4Digital Summit 2023).

Conclusions

The digital transformation of business in the Republic of Moldova is demonstrating steady growth, accompanied by the active implementation of various types of innovation. However, each innovation creates new vectors for cyberattacks. Along with technological progress comes a cause for concern: the growing gap between innovation and cybersecurity. According to the National Cybersecurity Center, 152 million cyber incidents were registered in 2023, and ransomware attacks increased by 85% (Raport-Strategie, 2024).

Organizations using open-source innovation and platform offerings are particularly vulnerable. At the same time, only 15% of small and medium-sized enterprises (SMEs) spend sufficient resources on security (IDIS,2025), posing a vital threat to the national economy. Statistics have shown that companies that invest in cybersecurity are 40% more resilient to crises (Cybersecurity in Moldova's SMEs,2025). To further improve the situation, all efforts should be focused on infrastructure development and the implementation of existing measures.

Business development in Moldova through digital technologies is becoming increasingly visible every day, but the gap between cybersecurity and innovation is enormous. Recent data shows that companies that invest in cybersecurity are 40% more resilient to crises.

Successfully overcoming cyber threats requires coordinated action by the government, businesses, and educational institutions. Cyber resilience should become a central aspect of business development policy in Moldova and the national economy as a whole, guaranteeing the safe implementation of digital innovations and sustainable economic growth.

Successful overcoming of cyber challenges is only possible through the joint efforts of the state, businesses, and educational institutions. Cyber resilience should be part of the development strategy of Moldovan businesses and the entire national economy as a security measure for the use of digital innovations and ensuring sustainable development.

References

1. Digital Economy and Society Index (DESI) 2023 https://digital-strategy.ec.europa.eu/en/policies/desi (Accessed 22 Jun e2024).
2. Cyber Threat Statistics in the EMEA Region 2023 https://www.kaspersky.ru/about/press-releases/kaspersky-ics-cert-v-2023-godu-znachitelno-vyroslo-chislo-incidentov-v-rezultate-kiberatak-na-promyshlennye-organizacii?ysclid=mgtuss7peh981122590 (Accessed 01 June 2025).
3. National Bureau of Statistics of the Republic of Moldova. https://statistica.gov.md/ru/statistic_indicator_details/18 (Accessed 01 July 2025).
4. Raport-Strategie, 2024 (Report of the Republic of Moldova Digital Transformation Strategy 2023-2030) https://mded.gov.md/wp-content/uploads/2024/05/EN_Raport-Strategie.pdf

5. Orange Moldova. https://www.orange.md/ru/business/cybersecurity (Accessed 01 July 2025).
6. State of cybersecurity in the EU | ENISA https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu (Accessed 01 August 2025).
7. Legea Nr. 48 din 16-03-2023 privind securitatea cibernetică https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro
8. IDIS | Institutul pentru Dezvoltare și Inițiative Sociale „Viitorul" (Accessed 21 August 2025).
9. World Bank. GDP per capita (current US$) | Data https://data.worldbank.org/indicator/NY.GDP.PCAP.CD (Accessed 01 August 2025).
10. National Cyber Security Index (NCSI). Moldova Report 2023 https://ncsi.ega.ee/country/md/188/ (Accessed 22 August 2025).
11. Global Cybersecurity Index https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (Accessed 21 August 2025).
12. UN E-Government Development Index https://desapublications.un.org/?keywords=cyber&sort_by=date&sort_order=DESC (Accessed 01 September 2025).
13. Cybersecurity in organizations of the United Nations system https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_russian.pdf(Accessed 01 August 2025).
14. Armas Reismary , Taherdoost Hamed Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm 2025 **https://doi.org/10.3390/info16050336** (Accessed 01 September 2025).
15. Network Readiness Index 2023 https://download.networkreadinessindex.org/reports/countries/2023/republic-of-moldova.pdf (Accessed 01 September 2025).
16. PISA. Cybersecurity dynamics in the Republic of Moldova: responding to complex threats. https://pisa.md/ (Accessed 01 September 2025).
17. HTTPCS Moldova,2024 Cyber Attack Map HTTPCS - Moldova https://map.httpcs.com/country/MD(Accessed 01 September 2025).
18. Activity of small and medium enterprises in the Republic of Moldova in 2023 (Accessed 01 September 2025).
19. National Bank of Moldova Payment Systems Report 2023 https://www.bnm.md/ru/tipuri-de-publicatii/rapor-privind-supravegherea-sistemului-de-plati-din-r-moldova (Accessed 11 September 2025).
20. Scoreboard, Consumer conditions scoreboard 2023 https://commission.europa.eu/system/files/2023-10/consumer_conditions_scoreboard_2023_v1.1.pdf (Accessed 11 September 2025).
21. Rusweb. Raport De Activitate 2023 Rusweb. https://datepersonale.md/wp-content/uploads/2024/03/raport_de_activitate_2023_rusweb.pdf (Accessed 11 September 2025).
22. Forbes. The Cybersecurity Crisis: Companies Can't Fill Roles, Workers Shut Out https://www.forbes.com/sites/emilsayegh/2025/02/05/the-cybersecurity-crisis-companies-cant-fill-roles-workers-shut-out/ (Accessed 11 September 2025).
23. IT in Innovation Technology Park MITP https://infomarket.md/ru/analitics/352976 (Accessed 01 September 2025).
24. EU4Digital at Moldova Digital Summit 2023 - EU4Digital https://eufordigital.eu/eu4digital-at-moldova-digital-summit-2023/ (Accessed 01 August 2025).
25. Cybersecurity in Moldova's SMEs: Findings from a national survey » E-riigi Akadeemia https://ega.ee/cybersecurity-survey (Accessed 01 September 2025).
26. Digital transformation of SMB in the Republic of Moldova https://ibn.idsi.md/sites/default/files/imag_file/328-335_1.pdf (Accessed 01 September 2025).