Problems and Solutions: Cybersecurity a Key Point in the Digitalization Stage for the Romanian Public Sector

Mircea-Alexandru Lungu[1]
[1)] *Bucharest University of Economic Studies, Bucharest, Romania*

E-mail: mircea.lungu@ie.ase.ro

Please cite this paper as:
Lungu, M.A., 2025. Problems and solutions: Cybersecurity a key point in the digitalization stage for the Romanian public sector In: C. Vasiliu, D.C. Dabija, A. Tziner, D. Pleşea, V. Dinu eds. 2025. *11th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Oradea, Romania, 26-28 June 2025. Bucharest: Editura ASE, pp. 150-157
DOI: 10.24818/BASIQ/2025/11/003

Abstract

This article analyses digital challenges and opportunities. Currently, in Romania, the Public Administration is at a crossroads, as it faces ups and downs in terms of digital transformation, especially in terms of cybersecurity but also the effects on employees. There is great potential for simplifying services, reducing bureaucracy, but currently we are faced with outdated IT systems, bureaucratic bottlenecks and an unskilled workforce unprepared for technological modernization. To analyse and find solutions to these problems, this study is based on a combination of existing research and insights from 136 interviews with public sector employees as well as IT experts and decision-makers in Romania. Using NVivo to analyse the data – sorting by themes and word patterns – presented a harsh reality of the current system: Romania's digital infrastructure is underfunded, systems rarely work well together, and cybersecurity issues are a constant concern. Bureaucracy exacerbates the problems, slowing down work even more, and many employees lack the technological skills needed to keep up. However, digitalization has massive potential to turn things around, provided it is accessible to all. This research brings a new vision of the growing complexity of digitalization in the Romanian public sector. Through an analysis of interviews and the use of NVivo, the study identifies non-religious points that influence the success of the transformation and proposes concrete strategies for stabilizing cybersecurity, increasing the skills of public sector employees, and optimizing digital public services. The findings of this study can be used as a guide for public sector leaders in developing policies and programs to develop the digital system and increase cybersecurity. Measures are proposed to increase the amounts allocated for investments in IT infrastructure, conduct employee training courses, stabilize national standards, and encourage public-private collaboration.

Keywords

Digital transformation, employee motivation, public institutions, digital leadership, adaptability, emerging technologies, organizational culture.

DOI: 10.24818/BASIQ/2025/11/003

Introduction

This shift toward digital systems is turning public institutions inside out, reshaping workflows, workplace culture, and what keeps employees motivated. Tools like artificial intelligence, automated processes, and cloud-based platforms promise to make operations smoother and more transparent (Westerman, Bonnet, & McAfee, 2019). The increased visibility of employee behaviours through digital tools can further influence workplace dynamics and motivation (Leonardi & Treem, 2020). Picture clerks breezing through tasks instead of wading through endless forms—it's a vision that can lift job satisfaction (Baptista et al., 2020). Picture clerks breezing through tasks instead of wading through endless forms—it's a vision that can lift job satisfaction (Baptista et al., 2020). But the road isn't easy. New tech can spark stress, pushback, or fears about job security (Vial, 2019). Success hinges on leaders who inspire and practical support like user-friendly training. This research dives into how digitalization shapes motivation in Romania's public sector, using interviews and NVivo analysis to capture employees' perspectives. The findings pinpoint what fuels engagement—or kills it—and offer ideas for helping workers embrace tech without feeling lost.

1. Research Methodology

This study uses a qualitative research approach to investigate the challenges and opportunities of digitalization and cybersecurity in public administration in Romania. The methodology is designed to capture in-depth perspectives of public sector stakeholders, combining empirical data collection with systematic data analysis to develop a comprehensive understanding of the issues at hand.

1.1 Data Collection

The data source for this study consists of 136 semi-structured interviews conducted with a diverse group of participants, including public sector employees, IT specialists and decision-makers in Romania. The interviews were conducted to gain an impression of employees' digital transformation, cybersecurity issues and the motivation of people in public administration. Participants were selected through purposive sampling, a qualitative selection that allowed individuals based on their relevance to the research subject. Selection criteria included: *function* (administrative employees, IT specialists, managers), *experience in similar projects* (cybersecurity and digitalization), and *being employed at various public institutions*, such as universities, city halls, and other local authorities. To ensure impartiality, the sample included participants from both urban and rural areas, from central and local institutions, as well as from various regions of Romania (including Bucharest, Oltenia, Moldova, and Muntenia). This distribution allowed for the capture of a broader range of perspectives on digitalization in the context of the institution to which the employees belong. In the selection process, participants were identified through contact and recommendations, followed by an assessment of eligibility according to the aforementioned criteria. The number of 136 interviews was determined based on thematic saturation, at which point recurring themes became evident and additional data no longer brought significant new insights. The interviews were conducted both in person and online, depending on the participants' time and the data collection method, and were fully transcribed to ensure data accuracy.

1.2 Data Analysis

The data collected from the interviews were analysed in NVivo. This was followed by a three-stage thematic coding process:

- **Open Coding:** First, a detailed analysis of the interviews was conducted to find themes and concepts. Each text unit was inductively labelled, resulting in the extraction of 10 primary thematic codes, such as cybersecurity, digital skills, and bureaucracy, as described in Section 3.
- **Axial Coding:** In the second stage, the links between the initial codes were established to form higher-level thematic categories.
- **Selective coding:** The last stage united the themes found in a unified theoretical framework, focusing on the interaction between digitalization, cybersecurity and employee engagement with a focus on cybersecurity.

2. Problems identified in cybersecurity in public administration and possibilities for improvement

Romania has made significant progress in the digitalization of public administration, yet the implementation process remains cumbersome and faces numerous obstacles. Although initiatives such as Ghișeul.ro, the Virtual Private Space (SPV) platform, or the implementation of electronic signatures in certain institutions are important steps in modernizing the digital infrastructure, multiple structural and operational deficiencies persist.

2.1 Outdated information systems and lack of interoperability

One of the main challenges faced by Romania's public administration is the use of outdated IT systems, which limit administrative efficiency and complicate the data integration process between ministries and agencies. The lack of interoperability between various platforms and databases leads to redundant bureaucratic procedures and increases the processing time for citizen requests. According to the Digital Economy and Society Index (DESI), Romania consistently ranked last in the digitalization of public services from 2016 to 2020, a trend that persists in more recent assessments (European Commission, 2023). This situation highlights the need for substantial reforms in the digital transformation of public administration. Low Interoperability – A Major Issue - There are multiple unsynchronized databases. For example, the healthcare system (CNAS) and the population records system do not communicate efficiently, leading to issues in issuing health cards.

2.2 Bureaucracy slows down digitalization

Although certain public services, such as the issuance of birth or marriage certificates, are available online, in many localities, citizens are still required to appear in person to collect documents. This requirement reduces the efficiency of the digitalization process and discourages the use of electronic solutions. The previously mentioned study also highlights that, although a draft law regarding the establishment of a national framework for interoperability in the IT field was launched for public consultation in 2019, it had not been implemented by 2020. This delay reflects the systemic difficulties encountered in adopting and implementing the necessary reforms for the modernization of public administration.

2.3 Deficient cybersecurity

Romania has faced multiple cyberattacks on public institutions, including the website of the Ministry of Defence, highlighting the vulnerabilities of digital infrastructure and the need for significant investments in IT security. The lack of adequate protective measures exposes citizens' data to major risks. In 2022, several government websites were targeted by cyberattacks, demonstrating the fragility of the digital systems used by public administration. Romania's performance in the Global Cybersecurity Index underscores the need for enhanced cybersecurity measures to address these vulnerabilities (International Telecommunication Union [ITU], 2023). These incidents underscored the necessity for robust cybersecurity solutions designed to prevent security breaches and unauthorized access to sensitive information. According to an article published by NOD Academy, although the process of digitizing public services has seen significant acceleration in the last two years, major challenges persist regarding the strengthening of technological infrastructure and the implementation of effective data protection mechanisms. The global rise in cyber threats, as highlighted in the Global Cybersecurity Outlook 2023, emphasizes the urgency for Romania to adopt advanced cybersecurity solutions (World Economic Forum, 2023). Ensuring adequate cybersecurity is an essential component for success. To better understand the risks and possible solutions, I conducted a qualitative study based on 136 interviews with representatives of public institutions, IT specialists, and decision-makers. The analysis carried out in NVivo highlighted the growing concern for data protection, the urgent need for investments, and the importance of national standards in information security. Additionally, the analysis of the frequency of words used by respondents revealed that the most mentioned terms were *'cybersecurity*,' *'security*,' *'data*,' '*institutions*,' and *'protocols*.' This finding confirms the importance of these aspects in the debate on cybersecurity and underscores the need for coherent and well-implemented measures to protect the digital infrastructure of public administration.

Figure no. 1. The analysis of the frequency of words used by respondents in the context of cybersecurity

The analysis of the interviews highlighted four major issues in the cybersecurity of public administration:

Table no. 1. Challenges and solutions in the field of IT security: An analysis of respondents' perceptions

Category	Identified Aspects	Percentage of Respondents (%)
Challenges	Insufficient investment in security	82%
	Shortage of qualified personnel	76%
	Unclear legislation and poor enforcement	54%
	Lack of advanced protective measures	35%
Proposed Solutions	Increasing investments in IT infrastructure	88%
	Organizing regular training sessions	76%
	Establishing strict national standards	67%
	Collaborating with the private sector	64%

Investment deficiencies in cybersecurity pose a major threat to the IT infrastructures of public administration, an aspect highlighted by data obtained from a qualitative study based on 136 interviews with representatives of public institutions, IT specialists, and decision-makers. The analysis of these interviews, conducted in NVivo, revealed three main themes: the growing concern for data protection, the urgent need for investments, and the importance of national standards in information security.

Specifically, the data coding was conducted according to the following thematic categories:

- Perception of cybersecurity (*n=112 respondents* mentioned concerns about cyberattacks and their impact on institutions);
- Factors hindering investments (*n=97 respondents* reported administrative and financial barriers to fund allocation);
- The necessity of a national strategy (*n=89 respondents* emphasized the importance of regulations that mandate a minimum budget for cybersecurity protection).

3. The analytical process of thematic coding using NVivo

The qualitative analysis of the data obtained through interviews conducted as part of the study on cybersecurity and the digitalization of public administration was based on a rigorous process of thematic coding, carried out in three distinct stages: open coding, axial coding, and selective coding. This methodological approach allowed for the extraction and structuring of significant data categories, ensuring not only a systematic classification of the identified aspects but also their integration into a coherent analytical framework.

3.1 Open Coding – Initial Identification of Relevant Categories

The initial stage of thematic coding involved a detailed fragmentation of the interview corpus, with each textual unit being analysed and classified according to the emerging themes. The coding process was conducted in an inductive manner, through the systematic labelling of participants responses and the identification of recurring thematic nodes. In this stage, 10 main codes were extracted and defined, reflecting the central issues of digitalization and cybersecurity in the public sector:

Table no. 2. Challenges and opportunities of digitalization in the public sector: Analysis based on respondents' perceptions.

No.	Thematic Code	Percentage of Respondents	Causes
1	Cybersecurity	82%	Lack of a coherent strategy for protecting digital infrastructures.
2	Impact of digitalization	72%	Structural and functional transformations in public administration.
3	Digital Skills	64%	Lack of staff training, an obstacle to optimizing digital services.
4	Benefits of digitalization	61%	Reducing bureaucracy, streamlining processes, better access to services.

5	Technical Challenges	58%	Low interoperability, difficulties in integrating digital infrastructures.
6	Legislation and digitalization	57%	Legislative gaps in regulating cybersecurity.
7	Project Financing	53%	Difficulties in obtaining and managing funds.
8	Bureaucracy and digitalization	49%	Procedural inefficiencies, complexity of public procurement.
9	Accessibility of Services	46%	Discrepancies in the use of digital technologies by different social groups.
10	Resistance to Change	41%	Manifested at the decision-making level and among administrative staff.

This stage provided a solid empirical foundation for developing a system of categories that allows for an in-depth interpretation of the data.

3.2 Axial Coding – Establishing Relationships Between Identified Categories and Grouping Them into Main Themes

Axial coding involved establishing relationships between the initial codes and grouping them into higher thematic structures that reflect the interdependencies and causal mechanisms among the identified factors. In this stage, network diagrams and interconnection matrices in NVivo were used, facilitating the analysis of correlations between the essential dimensions of digitalization and cybersecurity. To identify connections between themes, Matrix Coding Query was employed, an advanced relational analysis method that allows for examining the frequency of co-occurrences between codes, thereby indicating the degree of interdependence among the thematic variables identified during the coding process.

The results obtained from the matrix co-occurrence query highlighted four central dimensions in the process of digitizing public administration:

- Financing and implementation of projects (A);
- Legislation and digitalization (B);
- Technical challenges (C);
- Resistance to change (D).

Table no. 3. Relationships between the central dimensions of digitalization in public administration: Results of the matrix co-occurrence analysis

	Financing and implementation of projects	Legislation and digitalization	Technical challenges	Resistance to change
Financing and implementation of projects	272	0	136	136
Legislation and digitalization	0	159	0	0
Technical challenges	136	0	408	272
Resistance to change	136	0	272	408

For each of these, the **frequencies of co-occurrence** were analysed, providing **quantitative indicators** of the **intensity of the relationships** between the thematic concepts.

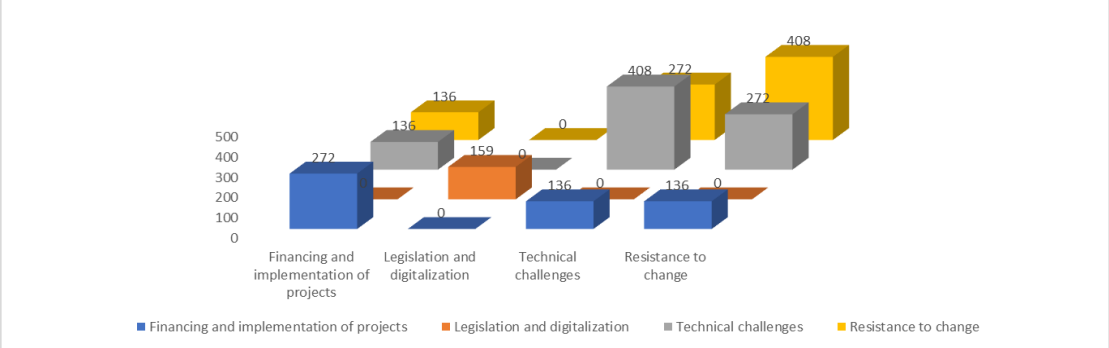

Figure no. 2. 3D representation of the relationships between the central dimensions of digitalization in public administration.

3.2.1. Relationship of themes between "Project financing and implementation" and other categories

- The most important relationship was identified between "Project financing and implementation" and "Technical challenges" (136 co-occurrences), and thus financial problems represent an important factor in their technical occurrence encountered in digitalization processes;
- An identical correlation (136 co-occurrences) is identified between "Project financing and implementation" and "Resistance to change", given that insufficient financial resources lead to reluctance towards digitalization, both at the structural and individual levels;
- The absence of a direct correlation between "Financing" and "Legislation and digitalization" (0 co-occurrences) shows that interview participants did not consider that regulatory aspects affect the possibility of accessing funds for the implementation of IT projects.

3.2.2 Legislation and digitalization – a domain seen as autonomous, without major interdependencies

This category registers a frequency of 159; However, it does not present co-occurrences with all the dimensions analyzed. This result shows that legislation is perceived as an independent element, which are not direct companies with financial, technical or resistance to change aspects.

3.2.3 Technical challenges – the dimension with the greatest impact on the digitalization process

- "Technical challenges" is the code with the highest total frequency of co-occurrence (408), indicating its central role in the NVivo analysis;
- The most important connections are with "Resistance to change" (272 co-occurrences), suggesting that technological difficulties are among the main factors hindering digital solutions;
- The interdependence with "Project financing and implementation" (136 co-occurrences) confirms that financial investments are an important factor in reducing technological difficulties.

3.2.4 Resistance to change – a dimension closely linked to technical challenges and financial resources

- "Resistance to change" shows the highest frequency of co-occurrence (408) with "Technical challenges", which shows that infrastructural deficiencies and the complexity of implementing IT solutions represent the main obstacles to digitalization;
- "Project financing and implementation" is also an associated factor of "resistance to change" (136 co-occurrences), confirming the impact of financial resources on the acceptance of digital transformation.

The relational analysis allowed the consolidation of three central themes:

1. Barriers and challenges in the digitalization of public administration
   - Associated Codes: bureaucracy and digitalization, digital skills of employees, resistance to change, financing and implementation of projects;
   - This theme reflects the systemic factors that hinder the effective implementation of digital technologies, including institutional deficiencies, competence gaps, and administrative obstacles.
2. Cybersecurity and IT infrastructure
   - Associated Codes: cybersecurity, technical challenges, legislation and digitalization;
   - This theme highlights the vulnerabilities of digital infrastructures, caused by underfunding, the lack of clear regulations, and difficulties in integrating modern technologies.
3. Benefits of digitalization and impact on citizens
   - Associated Codes: impact of digitalization, benefits of digitalization, accessibility of digital services for citizens;
   - This dimension emphasizes the transformative potential of digitalization, as well as the existing disparities in access to technology and digital public services.

Through this stage, a robust conceptual architecture was consolidated, capable of explaining the investigated phenomena within a coherent analytical framework.

3.3 Selective Coding – Integrating Major Themes into a Coherent Analysis

The final stage of the analysis involved organizing the main themes and integrating them into a coherent theoretical framework, which would explain the link between digitalization and cybersecurity in the context of public authorities. The analysis revealed that the digitalization of public administration is closely linked

to cybersecurity, administrative reforms and the development of digital skills of staff. Thus, a successful digital transformation requires a comprehensive approach, combining the use of new technologies with a well-regulated system prepared to face the current challenges.

3.3.1 Key Emerging Findings

The lack of a clear cybersecurity strategy increases the risk to IT systems. According to a study, 82% of respondents say that the lack of investment in cybersecurity leaves IT infrastructures vulnerable to major attacks. Moving from traditional methods of information protection to a more developed cybersecurity system is crucial to face current threats (Von Solms & Van Niekerk, 2013). Lack of funding and a lack of national regulations deepen these problems, preventing institutions from taking effective protective measures. In addition, dispersed responsibilities between institutions and the absence of a necessary framework for managing cyber incidents reduce the effectiveness of security systems. Although threats are becoming increasingly diverse and problematic, few public institutions use advanced technologies, such as artificial intelligence or behavioural analysis, to identify and prevent attacks. However, the adoption of these solutions varies widely, and the lack of expertise remains a major cause of strengthening cybersecurity.

Relational classification:

- *Associative Relationships:* Financing and implementation of projects ↔ Degree of digitalization;
- *One-way Relationships:* The lack of a coherent cybersecurity strategy → Increases → Vulnerabilities of IT Infrastructures;
- *Symmetrical Relationships:* Cybersecurity ↔ Citizens' trust in digitalization.

2. Bureaucracy and lack of employee skills slow down the adoption of new technologies

- 64% of respondents say that insufficient training of employees to use digital systems is a major problem in the transition to digitalization.
- 49% believe that rigid administrative procedures significantly block the implementation of new technologies, leading to delays and inefficiency in decision-making.
- Resistance to change and lack of compatibility between IT systems used by public institutions exacerbate the problems of the digitalization process.

To solve these problems, national training programs have been launched for public servants to help them adapt more quickly to new technologies. However, the impact of these programs is limited due to the lack of a strategy for developing digital skills and the frequent departure of already trained specialists from public administration.

Relational classification:

- *Associative relationships:* Bureaucracy and digitalization ↔ Legislation and digitalization;
- *One-way relationships:* Resistance to change → slows down → digitalization of public institutions;
- *Symmetrical relationships:* Digital skills of employees ↔ Productivity;

3. Digitalization brings substantial benefits, yet accessibility and digital equity remain major issues

- 72% of respondents acknowledged that digitalization has led to the optimization of administrative processes and increased institutional transparency;
- However, 46% indicated the existence of significant difficulties in accessing digital services, especially for vulnerable groups (the elderly, rural populations, individuals with disabilities);
- Disparities in digital infrastructure and low levels of digital literacy are factors that perpetuate inequalities in the use of digital technologies.

In an attempt to improve digital inclusion, digital platforms with optimized interfaces for users with limited skills and digital assistance services have been developed. However, inequalities persist, and effective access to digital services is conditioned by factors such as the level of digital education and the availability of IT infrastructure in disadvantaged areas.

Relational classification:

- *Associative relationships:* Cybersecurity ↔ Accessibility of digital services for citizens;

- *One-way relationships:* Technical challenges → Affects → Accessibility of digital services for citizens;
- *Symmetrical relationships:* Bureaucracy and digitalization ↔ Financing and implementation of projects.

The analysis shows that the digitalization of administration cannot succeed without a comprehensive approach that combines cybersecurity, administrative reforms, and developing digital skills.

Conclusions

The results of this empirical investigation reveal that the process of digital transformation of public administration in Romania is conditioned by a multitude of interdependent systemic factors, whose complexity requires a multidimensional approach and integrated public policies. To optimize the positive impact of digitalization and mitigate associated risks, the implementation of essential strategic measures is imperative: To make digitalization click, Romania needs a cybersecurity strategy that's ironclad, rooted in "security-by-design" and "privacy-by-default" principles to keep systems safe. That means investing heavily in top-tier tools—think cutting-edge intrusion detection, rapid incident response, and encryption that's tough to crack. Clear, strict laws are just as vital, laying out who's accountable and setting high bars for data protection. Regular security checkups ensure defences stay sharp against new threats. Beyond that, systems need to talk to each other seamlessly, which calls for standardizing data formats and using smart solutions like enterprise service buses or microservices. Automation through tools like BPM or AI can slash processing times and paperwork, while "lean management" ideas help cut through bureaucratic clutter for a nimbler administration. Most crucially, employees need to get tech-savvy through ongoing training in areas like cybersecurity, data analysis, or even basic coding. Creating dedicated training hubs and partnering with Romanian universities can spark innovation and build skills. Ultimately, transforming Romania's public administration into a digital success story demands bold strategies and tight collaboration across institutions. Done right, it could deliver a system that's fast, secure, and fair, offering better services to every citizen.

References

Baptista, J., Stein, M.-K., Klein, S., Watson-Manheim, M.B. and Lee, J., 2020. Digital work and organisational transformation: Emergent Digital/Human work configurations in modern organisations. *The Journal of Strategic Information Systems*, [online] 29(2), p.101618. https://doi.org/10.1016/j.jsis.2020.101618.

European Commission, 2023. *Digital Economy and Society Index (DESI) 2023*. [online] Available at: < https://digital-strategy.ec.europa.eu/en/policies/desi > [Accessed 13 March 2025].

International Telecommunication Union (ITU), 2023. *Global Cybersecurity Index 2023*. [online] Available at: < https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx > [Accessed 17 March 2025].

Leonardi, P.M. and Treem, J.W., 2020. Behavioral Visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, [online] 41(12), pp.1601–1625. https://doi.org/10.1177/0170840620970728.

NOD Academy, 2022**.** *Challenges of cybersecurity in the digitalization of public administration. NOD Academy Blog,* [online] Available at: < https://www.nodacademy.ro/blog/securitate-cibernetica-digitalizare > [Accessed 17 March 2025].

Smart Cities, 2020. *Digital economy and society Index (DESI) – Romania in the European context. Smart Cities Conference*, [online] Available at: < https://digital-strategy.ec.europa.eu/en/policies/desi > [Accessed 13 March 2025].

Vial, G., 2019. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, [online] 28(2), pp.118–144. https://doi.org/10.1016/j.jsis.2019.01.003.

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, [online] 38, pp.97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Westerman, G., Bonnet, D. and McAfee, A., 2019. *Leading Digital: Turning technology into business transformation. Harvard* Business Press.

World Economic Forum, 2023. *Global Cybersecurity Outlook 2023.* [online] Available at: < >https://www.weforum.org/reports/global-cybersecurity-outlook-2023/ > [Accessed 17 March 2025