

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

CYBERSECURITY IN MUNICIPAL ADMINISTRATIONS – RISKS, VULNERABILITIES AND OPPORTUNITIES FOR INCREASING RESILIENCE

Iliana K. Simeonova

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: i.simeonova@shu.bg

Abstract: *This paper examines cybersecurity in municipal administrations as a key component of administrative security and sustainable functioning of public services. The main cyber threats, vulnerabilities and factors affecting the level of protection of information resources are analyzed. Emphasis is placed on the management and assessment of cyber risk, the protection of critical information assets and the role of the human factor. An author's Model 5K for municipal cyber resilience has been developed, combining identification, assessment, protection, monitoring and resilience. The proposed approaches are aimed at incident prevention, effective response and restoration of municipal information systems and services.*

Key words: ***C****ybersecurity, Municipal administration, Cyber risks, Cyber threats, Vulnerabilities, Cyber resilience, Information security, Risk management, Human factor, Model 5K.*

1. Introduction

The digital transformation of the public sector significantly changes the way municipal administrations organize and carry out their management and administrative functions. The expansion of electronic administrative services, the use of information systems, digital registers and data exchange increase the efficiency and accessibility of administrative processes, but at the same time create new dependencies and prerequisites for the emergence of cyber risks. In this context, the security of information resources and the sustainability of digital infrastructure are becoming an essential condition for the normal functioning of municipal administration.

The increasing complexity and dynamics of cyber threats, combined with technological, organizational and human vulnerabilities, pose to municipalities the need for a systematic approach to cybersecurity management. Of particular importance is the ability of the administration not only to prevent cyber incidents, but also to identify them in a timely manner, to respond adequately and to restore critical administrative processes. Therefore, the cybersecurity of municipal administrations should be considered not only as a technical

problem, but as **a complex managerial, organizational and administrative-security problem** related to the sustainability of public administration.

The aim of this study is to analyze the main cybersecurity risks and vulnerabilities of municipal administrations and to propose a model for its sustainable management.

To achieve this goal, the following main tasks have been formulated: clarification of the specifics of cybersecurity in the municipal administration; identification of the main cyber threats and vulnerabilities; analysis of organizational and technological risk factors; assessment of the role of the human factor and development of an author's model for cybersecurity management.

2. Theoretical foundations of cybersecurity in municipal administration

2.1. Nature and characteristics of cybersecurity

Cybersecurity is a set of principles, policies, organizational and technical measures aimed at protecting information systems, network infrastructure, data and digital services from unauthorized access, violation of integrity, destruction, modification or blocking. In the context of accelerated digitalization, it becomes an essential component of the overall security of organizations and institutions, since the functioning of a number of management processes is directly dependent on the reliability and continuity of the information environment.

The classical principles of confidentiality, integrity and availability **of information are essential for cybersecurity**. Confidentiality implies the prevention of unauthorized access to information resources and data; integrity is related to preserving their accuracy, reliability and integrity, and availability – to ensuring timely and uninterrupted access to the necessary resources and services by authorized users. In the modern concept of security, these principles are complemented by the need for **resilience**, expressed in the ability of information systems and organizations to prevent, tolerate, respond to and restore their normal functioning after cyber incidents occur.

In this sense, cybersecurity should not be confined solely to the use of technical means of protection. It is a continuous management process involving the identification and assessment of risks, the identification of appropriate measures to limit them, access control, incident management, data backup and recovery, staff training and periodic updating of protection mechanisms.

2.2. Specifics of the municipal administration as an object of cyber threats

The municipal administration represents a specific environment from the point of view of cybersecurity due to the wide range of administrative activities, information resources and digital services that are maintained and managed at the local level. Within the framework of their powers, municipalities process significant volumes of information, including personal and identification data of citizens, information related to local taxes and fees, administrative proceedings, property relations, public procurement and financial transactions. This makes the information resources of the municipal administration a critical object for protection.

An additional factor for increasing cyber risk is the widespread use of *electronic administrative services, digital registers, document management systems and specialized information systems*, through which the interaction between the administration, citizens, business and other public institutions is carried out. The integration of municipal systems with national information resources and registers further increases the interdependence between the individual elements of the public digital infrastructure.

The specifics of the municipal administration are also determined by the need to ensure both *the accessibility of services and a high level of information protection.* Violation of the accessibility of a system, compromise of personal data or unlawful alteration of information

can lead not only to technological and financial consequences, but also to interruption of administrative processes, hinder the service of citizens and violation of trust in institutions.

Limitations in terms of the financial, human and technological capacity *of some municipal administrations are also essential. The shortage of specialized cybersecurity experts, limited resources for modernizing the information infrastructure and the need to maintain legacy information systems can create additional vulnerabilities. Along with technological factors, the human factor remains a significant source of risk – insufficient awareness, errors in working with information resources and non-compliance with established security rules can compromise even the best designed technical protection mechanisms.*

Therefore, the cybersecurity of the municipal administration should be considered as *a multicomponent system* in which technological means, organizational procedures, regulatory requirements, human factors and risk management function in interdependence. It is this interdependence that determines the need for an integrated approach, oriented not only to the prevention of cyberattacks, but also to building an overall capability for the sustainable functioning of the municipal administration in the event of cyber incidents.

3. Major cyber threats and vulnerabilities in municipal administrations

The digitalization of administrative processes expands the opportunities for the provision of public services, but at the same time increases the area of impact from cyber threats. The specifics of municipal administrations are determined by the presence of multiple interconnected information systems, different categories of users, data exchange with external institutions and providers, as well as the need for constant availability of electronic services. Therefore, the occurrence of a cyber incident should be considered not only as an information security breach, but as a potential factor for interruption of administrative processes and a decrease in institutional resilience.

3.1. Main types of cyberattacks

Among the most significant threats to municipal administrations, **ransomware** stands out - a type of malware that blocks access to information resources, most often by encrypting data, and subsequently making a ransom demand. The specific risk for municipal administration stems from the fact that the compromise of a system can affect related administrative processes, document flow, registers, and the provision of electronic services.

Phishing and spear-phishing attacks are **a particularly widespread prerequisite for successful cyberattacks**. Phishing uses electronic messages, links, files or other means of communication to obtain identification data or mislead the employee to perform an action providing access to the information environment. And in spear-phishing, the approach is more targeted, and the content of the attack can be adapted to a specific employee, position or administrative function.

Also a significant risk is the *compromise of user accounts* through stolen passwords, reused credentials, lack of multi-factor authentication, or other authentication mechanisms. Acquiring legitimate user rights can allow an attacker to remain undetected in the system and gain access to information or functionalities that are inaccessible to an external user.

The main threats should also include various forms *of malware*, exploitation of software vulnerabilities, unauthorized access and attacks on publicly available electronic services. Social *engineering*, which uses psychological and communication techniques to manipulate employees in order to obtain information or perform a certain action, is also of particular importance.

An additional risk factor is supply *chain attacks.* Municipal administrations use products, services and information solutions provided by external suppliers and contractors. Compromising such an external component or its insufficient protection can create an opportunity for penetration into the information environment of the administration, thus gradually expanding the boundaries of cybersecurity beyond the immediate control of the municipality.

3.2. Main vulnerabilities

The effectiveness of a cyberattack depends not only on the means used by the attacker, but also on the presence of vulnerabilities in the information and organizational environment. In the municipal administration, these vulnerabilities are complex in nature and can be conditionally systematized into several main groups.

VULNERABILITY GROUP	MAIN MANIFESTATIONS
Technological	Outdated software and hardware, unpatched systems, insufficient network segmentation, and inadequate endpoint protection
Organizational	Lack of or insufficiently updated security procedures, unclear allocation of responsibilities, and inadequate preparedness for incident response
Human Resources	Shortage of qualified specialists, insufficient professional competence, and limited opportunities for specialized cybersecurity training
Financial	Limited budgets for modernization, maintenance, specialized software, and cybersecurity services
Management	Insufficient control, monitoring, and cyber-risk assessment; lack of an integrated management approach
Human	Phishing attacks, use of weak or reused passwords, errors in information processing, and non-compliance with security policies and procedures
External	Dependence on suppliers, external contractors, cloud services, and integrated information systems

A technologically protected system can remain at risk if the security rights are misconfigured, insufficient control or the actions of an unprepared user. Similarly, the availability of qualified personnel cannot fully compensate for the use of outdated infrastructure or the lack of effective monitoring. Therefore, cyber resilience is the result of the **combined action of technological, organizational, personnel, financial and human factors**, and not of a separate protective measure.

3.3. The human factor as a critical vulnerability

Among these factors, the human factor occupies a special place, since the employee is both a user of the information system and a potential point of its compromise. The technical protection of the municipal information infrastructure can be compromised through an illegally opened file, a password used or sensitive information submitted. Therefore, even the availability of modern technical means does not guarantee a sufficient level of security if the organizational culture and user behavior are not compliant with the requirements for cybersecurity.

The risk associated with the human factor should not be understood solely as the result of negligence or insufficient competence. It is also related to the way in which administrative processes are organized, responsibilities are distributed and access to information resources is controlled. In this sense, individual error is often a manifestation of a wider organisational deficit.

Especially risky are situations in which the employee has broad access rights, uses the same password in different systems, does not recognize an attempt at social engineering, or does not have sufficiently clear rules for acting in case of a suspicious message, file or request. The occurrence of such an event can be the starting point of a chain of follow-up actions – compromising an account, accessing an internal information system, extracting or modifying data, and disrupting the functioning of administrative services.

Hence the need to include the human factor in cyber risks management not only through periodic training, but also through building a **sustainable culture of information and cybersecurity**. It implies clearly formulated rules, regular training of employees, control of access rights, mechanisms for reporting incidents and the formation of behavior in which security is perceived as part of the daily performance of official duties.

In addition, staff development should not be limited to current cybersecurity practices, but should also foster competencies for the critical and secure use of emerging digital technologies [19].

In this context, the understanding that the human factor has a **dual meaning** can be justified – it can be a source of vulnerability, but at the same time it is a key resource for early recognition, prevention and limitation of cyber threats. An employee who recognizes a phishing message, promptly signals unusual activity or follows established procedures turns from a potential vulnerability into an active element of the protection system.

Therefore, the resilience of the municipal administration to cyber threats requires a change from a model based mainly on **technical protection** to a model of **integrated cyber risk management**, in which technologies, organizational procedures, management mechanisms and the human factor are considered as interrelated components of a unified security system. It is this statement that creates a theoretical and practical basis for the development of a model for sustainable cybersecurity management in the municipal administration.

4. Cyber risk management in municipal administrations

Effective counteraction to cyber threats in municipal administrations requires a transition from a reactive to a proactive management model, in which potential risks are identified and assessed before an incident occurs. In this context, cyber risk management should be seen as a continuous process of identifying critical assets, identifying threats and vulnerabilities, assessing probability and impact, determining the acceptable level of risk and choosing adequate measures to mitigate it.

4.1. Identification and assessment of cyber risk

The initial stage of cyber risk management is related to the identification of information assets, the compromise of which could disrupt the functioning of the municipal administration. The next step is to identify potential threats and existing vulnerabilities that can be used to implement the respective threat.

Methodologically, the process can be represented by the sequence:

Asset → Threat → Vulnerability → Probability → Impact → Risk → Measure

In this approach, *an asset* is an information resource, system, infrastructure or service whose normal functioning is relevant to the administrative process. *A threat* is defined as a potential event or action that can cause a security breach, while *a vulnerability* is a weakness in the system, process or behavior that can be exploited by the threat concerned.

The risk assessment should take into account two main parameters – *the likelihood* of the threat materializing and the potential impact on the administration. *The impact* can manifest itself through loss of confidentiality, violation of the integrity or inaccessibility of information and services, as well as through financial, administrative, legal and reputational consequences.

On this basis, appropriate *risk management measures* can be determined – prevention, reduction, transfer or acceptance in the presence of a justified acceptable level. It is an important principle that the measures are tailored to the specific risk, and not to be applied formally and regardless of the actual degree of exposure of the administration.

4.2. Critical information assets

Effective cyber risk management implies a clear identification and categorization of information assets. In the municipal administration, they can be systematized into several main groups:

1. **information systems** – systems for management and processing of administrative information;
2. **databases** – containing personal, administrative, financial and other categories of information;
3. **registers** – electronic registers maintained in connection with the administrative functions of the municipality;
4. **electronic administrative services** – digital platforms and services through which the interaction with citizens and organizations is carried out;
5. **communication infrastructure** – network devices, servers, communication channels and related technical resources;
6. **document management systems** – means for creating, processing, storing and exchanging administrative documents;
7. **archives and backups** – resources that ensure the restoration of information and administrative processes;
8. **User accounts** – identification means through which employees gain access to information resources.

Not all assets have the same degree of criticality. It is therefore necessary to assess them according to their importance for the continuity of administrative processes. Those assets whose compromise would lead to a significant disruption of the provision of administrative services, loss or misrepresentation of sensitive information or the inability to perform key functions may be defined as critical.

Such a classification allows the limited resources of the municipal administration to be directed as a priority to the protection of assets of the highest importance. In this way, cybersecurity management is transformed from a general activity to protect the information environment into *targeted management of critical resources and related risks.*

4.3. Prioritization of risks

The identification of multiple cyber risks puts the need to prioritize them. Municipal administration usually functions with limited financial, human and technological resources, which is why it is not possible to treat all risks simultaneously with the same intensity. This requires the use of criteria to determine which risks require immediate intervention and which can be managed at a later stage.

A practical approach is the use of a **risk matrix** based on the ratio between the likelihood of a threat materializing and the potential impact on information assets and administrative processes:

PROBABILITY × IMPACT = LEVEL OF CYBER RISK

For the purposes of the analysis, the probability and impact can be evaluated on a five-point scale – from 1 (very low) to 5 (very high). The obtained value allows for the conditional separation of low, medium, high and critical risk.

The matrix should not be seen as a stand-alone management decision-making tool, but as a means of *structuring and prioritizing risk information*. High or critical risk requires faster identification and implementation of safeguard measures, while measures with a longer horizon can be applied to low risks.

The cyber risk environment is dynamic – new vulnerabilities appear, technologies change, new electronic services are introduced and dependencies on external providers are changing. Therefore, risk assessment cannot be a one-time administrative action, but must be part of *a constant cycle of risk identification, assessment, treatment and monitoring.*

From this point of view, cyber risk management in municipal administration can be presented as a continuous management cycle:

IDENTIFY → EVALUATE → PRIORITIZE → PROTECTIVE MEASURES → MONITORING → REEVALUATION

This approach creates an opportunity for limited resources to be directed to the most significant risks and at the same time lays the foundation for building resilience – the ability of the municipal administration to maintain its critical functions, respond to cyber incidents and restore the normal functioning of its information systems and services in a timely manner.

5. AUTHOR'S MODEL FOR CYBERSECURITY MANAGEMENT IN THE MUNICIPAL ADMINISTRATION

The analysis of the main cyber threats, vulnerabilities and risks shows that effective cybersecurity management in the municipal administration requires a systematic approach that combines the identification of critical resources, risk assessment, the implementation of protective measures, constant monitoring and the ability to respond and recover. On this basis, an author's **"Model 5K for municipal cyber resilience"** is proposed, through which cybersecurity is considered as a dynamic and continuous management process.

The proposed model includes five interrelated components:

K1 – CYBER IDENTITY → K2 – CYBER ASSESSMENT → K3 – CYBER DEFENSE → K4 – CYBER MONITORING → K5 – CYBER RESILIENCE → NEW ASSESSMENT

The main feature of the model is its cyclicity. It assumes that cybersecurity management does not end with the introduction of protective measures. The results of monitoring, incidents that have occurred and changes in the information environment should lead to a re-identification and assessment of the risk.

The first component of the model is Cyber **Identification** – a systematic process of identifying information assets, critical administrative processes, dependencies between them and existing vulnerabilities.

In this phase, it is determined what needs to be protected and which resources are of key importance for the functioning of the administration. Information systems, databases,

electronic registers, administrative services, communication infrastructure, document management systems, archives and user accounts are identified. Along with the assets, critical administrative processes are also identified, the interruption of which would have a significant impact on the service of citizens and the performance of the functions of the municipality.

Of particular importance is the identification of *dependencies* – between individual information systems, between municipal administration and national information resources, as well as between the administration and external suppliers, thus forming a comprehensive picture of the digital environment and its potential points of vulnerability. The result of **K1** is an up-to-date profile of information assets and critical processes, which serves as a basis for the subsequent risk assessment.

The second component, **Cyber Assessment**, aims to determine the degree of exposure of the identified assets and processes to various cyber threats. Within this stage, the probability of a threat materializing, the potential impact, the criticality of the affected asset and the acceptable level of risk are assessed. Cyber assessment allows risks to be compared and prioritized, thus creating a basis for identifying those areas where immediate or priority protective actions are needed. It is important that the assessment covers not only technical parameters, but also organizational, personnel and human factors.

The **K2** outcome is a structured picture of cyber risk, including the identified risks, their extent and priority for treatment.

The third component – **Cyber Protection**, is the practical implementation of measures to mitigate the identified risks. The protection should be complex in nature and include technical, organizational and human mechanisms. Technical measures can include protection of end devices, network access control, software updates, network segmentation, cryptographic mechanisms, information redundancy and means of detecting malicious activity. Of particular importance is the principle of minimum *necessary access rights*, in which each user receives only those rights that are necessary for the performance of his or her official functions. In addition, data protection and redundancy of critical systems create prerequisites for limiting the consequences of a successful attack. The result of **K3** is to reduce the identified vulnerabilities and limit the likelihood and impact of the identified risks.

The fourth component, **Cyber Monitoring**, provides constant observability of the state of the information environment. It includes monitoring of systems, logging events, activity analysis, detection of anomalies and early warning of potential incidents. The importance of this component stems from the dynamic nature of cyber threats. Even in the presence of pre-implemented protective measures, it is possible for new vulnerabilities to appear or change in the behavior of attackers. Therefore, cybersecurity cannot be based solely on preventive mechanisms. Cyber monitoring creates an opportunity for *early detection of deviations from normal behavior*, which can shorten the response time and limit the potential impact on administrative processes. The registered information should be used not only for operational response, but also as a basis for subsequent analysis and improvement of defense mechanisms. The result of **K4** is increased observability and the ability to timely identify potential cyber incidents.

The fifth component, Cyber **Resilience**, is the ability of the municipal administration to maintain or restore its critical functions in a timely manner when a cyber incident occurs. Unlike the traditional model, which focuses primarily on the prevention of attacks, cyber resilience accepts the possibility of an incident and focuses on the organization's ability to *respond, limit impact, restore services and learn lessons from the event*.

This component includes incident response procedures, business continuity plans, data backup and recovery, recovery of critical information systems and subsequent analysis of causes and consequences. It is particularly important that the results of the incident analysis

are used to prevent its recurrence or to limit its impact in future similar events. In this way, **K5** performs the function not only of response and recovery, but also of an organizational learning mechanism, where the connection between the experience gained and the next risk management cycle is made.

The figure 1 shows that the five components do not function in isolation, but form an interconnected system. Cyber identification determines the object of protection, cyber assessment determines its degree of exposure to risk, cyber protection introduces the necessary measures, cyber monitoring tracks their effectiveness, and cyber resilience provides the ability to respond and recover.

The essential feature of the model is *feedback*. Changes in the information environment, new vulnerabilities, identified anomalies and the results of real cyber incidents should lead to a new identification and reassessment of the risk. In this way, the model acquires an adaptive character and allows the municipal administration to develop its security mechanisms in accordance with the changing environment.

In this sense, the **"5K Model for Municipal Cyber Resilience"** offers an integrated framework in which *security is considered not as a static state, but as a continuous process of identification, evaluation, protection, monitoring, response and improvement.* Its practical applicability is expressed in the ability for individual components to be adapted to the size, resources, information infrastructure and specific risk profile of each municipal administration.

Figure 1. Model 5K for Municipal Cyber Resilience

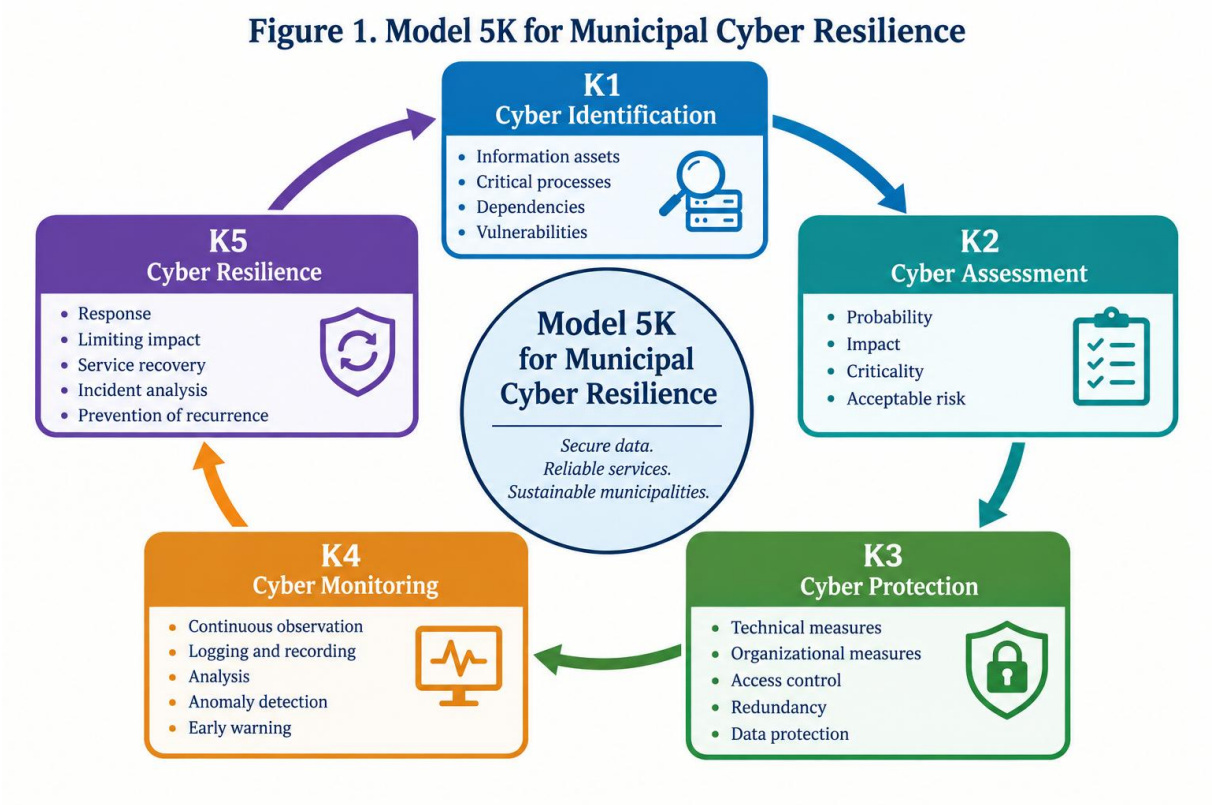


Fig. 1. New cyber assessment and model update

6. REGULATORY AND INSTITUTIONAL FRAMEWORK

The cybersecurity of municipal administrations is developing in the context of a multi-level regulatory and institutional framework that combines European and national requirements. Directive (EU) 2022/2555 – NIS2 is essential in the European context, aimed at achieving a high common level of cybersecurity in the European Union. The directive introduces a wider scope of regulated entities, risk management requirements, incident reporting, organizational measures and institutional interaction. With regard to public administration, it provides for the inclusion of certain administrative entities, and Member States can extend the scope to local administration as well.

In Bulgaria, the Cybersecurity Act **is of key importance**, which regulates the organization, management and control of cybersecurity and defines the main obligations for the entities within its scope.

A particularly significant change occurs with the amendments **promulgated in the State Gazette No. 17 of 13 February 2026**, which introduce the requirements of NIS2. According to the current framework, municipalities are included as administrative bodies and are defined as **"essential entities",** which puts cybersecurity in direct connection with the managerial responsibility of the municipal leadership.

The General Data Protection Regulation (Regulation (EU) 2016/679 – GDPR) has direct application and sets requirements for the security of processing, technical and organizational measures and the protection of the rights of individuals. This is particularly significant for municipal administrations due to the large volume of personal data they process within the framework of administrative services.

Another essential regulatory component is the **e-Government Act**, which regulates the work of administrative authorities with electronic documents, the provision of administrative services electronically, the exchange of electronic documents and the maintenance of electronic registers. Therefore, cybersecurity cannot be separated from the requirements for the functioning of e-government, as the security, accessibility and reliability of digital administrative services are interlinked.

In institutional terms, the municipal administration functions as part of a national cybersecurity system, which implies interaction with the competent state authorities and structures for the prevention, detection and management of cyber incidents. This interaction is especially important in incidents that exceed the technical capacity of a particular municipality or have the potential to affect interconnected information systems.

Therefore, the regulatory framework should not be seen as a set of formal obligations, but as a *basis for building a governance system for cyber resilience*. Its practical importance is manifested precisely through the transformation of regulatory requirements into specific policies, procedures, risk management mechanisms, control and continuous improvement.

7. Recommendations for increasing cybersecurity

Increasing cybersecurity in municipal administrations requires a combination of technological, organizational and management measures. Based on the analysis carried out, the following main directions can be formulated:

1. **Development and periodic updating of a municipal cybersecurity policy related** to the specific functions, information assets and risk profile of the administration.
2. **Periodic cyber risk assessment**, including the identification of critical assets, vulnerabilities, potential threats and possible consequences.

3. **Systematic employee training and cyber hygiene development**, with an emphasis on phishing recognition, social engineering, secure password management and incident response rules.
4. **Introduction of multi-factor authentication** for critical systems and user accounts, especially when remote access and access to sensitive information.
5. **Regular backup and recovery of data**, including periodic testing of the ability to recover critical information resources.
6. **Develop and update cyber incident response plans**, including clear responsibilities, communication channels and procedures for the recovery of administrative services.
7. **Periodically conduct tests, audits and security assessments** to identify emerging vulnerabilities and weaknesses in the applied security mechanisms.
8. **Continuous monitoring of critical information systems**, allowing early detection of anomalies and potential cyber incidents.
9. **Strengthen control over external suppliers and contractors**, including by defining security requirements in contractual relationships and assessing supply chain risks.
10. **Building a sustainable organizational culture of cybersecurity**, in which the protection of information resources is perceived as the responsibility of the entire administration, and not only of IT specialists.

These strands should be considered as an interconnected system. Their effective implementation implies management commitment, adequate resource allocation and periodic reassessment of the results achieved. In this way, cybersecurity can be integrated into the overall management process of administrative security and resilience.

8. Conclusion

The accelerated digitalization of municipal administrations creates significant opportunities to increase the efficiency, accessibility and quality of public services, but at the same time expands the digital surface for the impact of cyber threats. Dependence on information systems, electronic registers, digital services and integrated information resources makes cybersecurity an essential component of the sustainable functioning of local administration.

The analysis carried out shows that cyber risks in the municipal environment are complex in nature and arise from the interaction between technological, organizational, personnel, financial and human factors. Therefore, their management cannot be based solely on technical means of protection. It is necessary to build a comprehensive management system based on the identification of critical assets, assessment and prioritization of risks, the implementation of adequate protective measures, constant monitoring and readiness for response and recovery.

In this context, the proposed **"Model 5K for Municipal Cyber Resilience"** brings together five interrelated areas – cyber identification, cyber assessment, cyber defense, cyber monitoring and cyber resilience. Its main characteristic is the cyclical nature, in which the results of monitoring and response to incidents are used for a new assessment and update of security measures.

Therefore, the cybersecurity of the municipal administration should not be *reactive, but preventive; not only technical, but managerial; not one-time, but constantly evolving; not isolated, but integrated into the overall system of administrative security. It* is this approach that creates prerequisites for increasing the cyber resilience of municipalities and for ensuring the continuity, reliability and security of public services in a dynamic digital environment.

References

[1] Cybersecurity Act. Promulgated SG No. 94 of 13.11.2018, with subsequent amendments and supplements.

[2] Law on Amendment and Supplement to the Cybersecurity Act. State Gazette, No. 17 of 13.02.2026.

[3] Electronic Government Act. Promulgated SG No. 46 of 12.06.2007, with subsequent amendments and supplements.

[4] Personal Data Protection Act. Promulgated SG No. 1 of 04.01.2002, with subsequent amendments and supplements.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR).

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

[7] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity, 2025.

[8] European Union Agency for Cybersecurity (ENISA). ENISA Sectorial Threat Landscape: Public Administration 2024. European Union Agency for Cybersecurity, 2025. The report analyses 586 publicly reported cyber incidents in public administration in 2024 and identifies public administration as one of the most heavily attacked sectors in the EU.

[9] European Union Agency for Cybersecurity (ENISA). NIS360 2024. European Union Agency for Cybersecurity, 2024.

[10] European Union Agency for Cybersecurity (ENISA). Cybersecurity Guidelines for SMEs. European Union Agency for Cybersecurity.

[11] Schmidt, J. M., Mahula, S., & Crompvoets, J. (2025). Lessons Learned for Local Cybersecurity: Practical Implications of a Public Sector Cyberattack for Small and Medium-Sized Municipalities. Conference on Digital Government Research. DOI: 10.59490/dgo.2025.994. The study is particularly relevant to this topic, as it examines the practical consequences of a ransomware attack against an IT provider serving more than 70 municipalities and highlights the importance of network segmentation, monitoring and two-factor authentication.

[12] Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 3rd ed. Syngress.

[13] Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. 7th ed. Cengage.

[14] Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. 4th ed. Pearson.

[15] Krebs, R. (2021). Cybersecurity: A Practical Approach. Wiley.

[16] International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
[17] International Organization for Standardization (ISO). (2022). ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls.
[18] National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg: NIST.
[19] National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: National Institute of Standards and Technology.
[20] Tasinov, T. Y., Toncheva, S. K. Anticipatory Technological Preparation and Digital Health Competencies in Nursing and Midwifery Education. In: Conference Proceedings, XIX National Forum of Health Care Specialists and Poster Session for Students „Fair Access to Quality Health Care“, Shumen, 24–25 October 2025, pp. 97–103.