BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

On Cyber Vulnerabilities Management in Critical Sectors: the Health Sector

Irina-Delia NEMOIANU, PhD*
*Romanian National Cyber Security Directorate
e-mail: irina.nemoianu@dnsc.ro

Abstract

The digitalisation of the Romanian health sector has accelerated significantly, especially in the aftermath of the COVID-19 pandemic, but this transition has amplified cybersecurity risks, exposing critical infrastructures and patient data to persistent threats. This study analyses the technical and non-technical vulnerabilities of the medical sector, based on both documentary research and a survey conducted among representatives of health institutions. The results highlight important challenges, ranging from the use of outdated software, shortages of specialised cybersecurity staff and significant variations in the level of maturity of cyber protection between public and private organisations. Given the diversity of challenges identified, the resilience of the health sector requires an integrated cybersecurity strategy, underpinned by technological investments, continuous training and coherent risk management policies.

Keywords:
cybersecurity; cyber-attacks; vulnerabilities; the health sector; resilience; the human factor.

Article info
Received: 31 March 2025; Revised: 29 April 2025; Accepted: 6 May 2025; Available online: 27 June 2025

Citation: Nemoianu, I.D. 2025. "On Cyber Vulnerabilities Management in Critical Sectors: the Health Sector". *Bulletin of "Carol I" National Defence University*, 14(2): 247-256. https://doi.org/10.53477/2284-9378-25-27

In a global context marked by technological advances, the digitalisation of the healthcare system has become a strategic priority for Romania, aiming to improve the quality and efficiency of healthcare services. This has been accelerated by the COVID-19 pandemic, which highlighted the need for the medical sector to adapt quickly to the new realities. However, the sector faces significant challenges in terms of cybersecurity, both in terms of infrastructure and human resources expertise.

Increased digitisation has led to the expansion of the attack surface for cyber threats, evidenced by the increasing number of cyberattacks on the Romanian healthcare system. The RO-CCH project (RO-CCH 2025a), funded by the European Union and implemented by the Romanian National Cyber Security Directorate (DNSC), addresses cybersecurity challenges in the health sector, with the aim of reducing cybersecurity risks and raising awareness in health institutions in Romania.

Based on the work carried out within the project, this article presents an analysis of cybersecurity vulnerabilities that can affect the health sector in Romania, highlighting the socio-technical dimensions. These dimensions reflect the interactions between technical components - hardware, software and network infrastructure - and social factors - such as human behaviour, organisational culture and the regulatory framework, and the need for an integrated approach to achieving the resilience of the sector. The study also integrates the results of a survey conducted with hospital representatives, highlighting their perception of cyber threats and the current capacity of organisations to manage vulnerabilities.

Cyberattacks on the health system

The Romanian healthcare system is facing a significant increase in cyber threats, especially ransomware attacks, targeting both hospital IT infrastructures and IT service providers in the field. These trends are in line with European or global trends (ENISA 2023), where 8% of ransomware attacks in 2023-2024 targeted the health sector, the third most affected sector (ENISA 2024, 15). In Romania, the attacks demonstrated vulnerabilities in both data protection and continuity of regular operations, underlining the need for robust cybersecurity measures and recovery plans in case of an incident.

In July 2021, Witting Clinical Hospital No. 1 in Bucharest was the victim of a ransomware attack with the Phobos malware, which encrypted data on the institution's servers, with attackers demanding a ransom for decryption (SRI 2021). This ransomware, usually distributed by exploiting Remote Desktop Protocol (RDP), remote access vulnerabilities in Windows operating systems, functions as a Ransomware-as-a-Service (RaaS) platform (Cisco Systems Inc. 2023). Such platforms allow collaboration between developers and affiliates to extend attacks. The decentralised nature of the model makes it difficult to identify attackers and apply

countermeasures, and although the Romanian Intelligence Service (SRI) has provided recommendations for securing the IT infrastructure, the extent of the damage has not been made public. A similar incident occurred in 2023 at the 'Saint George' Recovery Hospital in Botosani, where the attackers encrypted the institution's database, seriously disrupting the activity and demanding a ransom of three bitcoins (approximately EUR 50,000) (ProTV 2023). This intensely publicised attack highlighted the severe impact of cyber threats on the Romanian healthcare system.

The latest large-scale ransomware attack took place between 11 and 12 February 2024, affecting Romanian Soft Company, the provider of the Hippocrates IT platform used by many public hospitals in Romania (DNSC 2024). The incident severely disrupted the work of 26 hospitals that depended on this platform for data management and coordination of medical services. The malware used was Backmydata, a variant of Phobos ransomware, similar to the one used in the 2021 attack on Clinical Hospital No. 1 Witting. At the time of writing, the exact cause of the incident was not publicly disclosed, but the DNSC noted that no evidence of data exfiltration had been identified. Thus, it remains uncertain whether the attack exploited a vulnerability of the platform, an erroneous configuration of the RDP or other human errors.

The increase in the frequency and complexity of ransomware attacks on the IT infrastructure in the Romanian medical sector highlights the risks associated with deficiencies in cybersecurity and supply chain vulnerabilities. Recent attacks highlight the need to implement strategies to protect hospital networks, including implementing strict data backup and recovery policies to prevent losses from ransomware attacks, protecting computer services exposed to the internet, or connecting to internal networks through secure Virtual Private Network (VPN) connections. Other measures that ensure resilience in case of materialised attacks can be increased investments in advanced cybersecurity solutions and rapid incident response plans, as well as training IT and medical personnel to detect and prevent common cyber threats, starting with phishing.

Cyber vulnerabilities

In cybersecurity, vulnerabilities are structural weaknesses or errors in computational logic identified in software or hardware components that, when exploited, may compromise the confidentiality, integrity and availability of data and information systems. These weaknesses can result from design, implementation or configuration deficiencies and are access points for attackers.
Mitigating these vulnerabilities usually involves one or more of the following measures:

- Applying patches to fix errors in the code
- Modification of the technical specifications so as to reduce exposure to potential operations

• Impairment or complete removal of functionalities or protocols that present vulnerabilities

According to the Common Vulnerabilities and Exposures (CVE) programme (The MITRE Corporation n.d.; SecurityScorecard n.d.), managed by MITRE Corporation, each vulnerability is recorded under a unique CVE ID, which allows it to be associated with specific versions of the software or shared libraries, thus providing a reference system to assist in the vulnerability management process.

The Common Vulnerability Scoring System (CVSS) (NIST n.d.) provides a metric for assessing the severity of cybersecurity vulnerabilities based on several criteria such as their impact and exploitability. It can be translated into a qualitative representation (low, medium, high and critical) to help organisations assess and prioritise vulnerabilities in management processes. CVSS is a public standard developed by the Special Interest Group (SIG) and widely used by organisations around the world, the latest version being CVSS 4.0. Hospital IT systems can face numerous cyber vulnerabilities, many of which affect various hardware, software and network products widely used in other sectors, which can compromise patient data security and the functioning of critical healthcare infrastructure.

Following documentary research and discussions with cybersecurity experts working with health entities, the most common problems identified include the use of outdated software and hardware, exposed to risks due to a lack of updates and adequate technical support. Poor network security protocols, poor configurations and inadequate access control measures can also facilitate unauthorised access to computer systems. In addition, insufficient training of medical and administrative staff increases the vulnerability of health institutions to phishing attacks, which remain one of the main methods of compromising IT infrastructure. These shortcomings expose hospitals to significant threats such as data breaches, ransomware attacks and unauthorised access to sensitive information, underlining the need to implement effective and proactive cybersecurity measures.

The report (RO-CCH 2025b) outlines a number of cyber vulnerabilities related to hardware, software, network equipment or cybersecurity equipment that healthcare organisations can consider in their security strategies. In this context, certain vulnerabilities identified by the corresponding CVEs, whether historical or newly discovered, present a high (High) or critical (Critical) CVSS score that requires an urgent approach and effective mitigation measures, given the potential impact on the continuity of health services and the protection of critical infrastructure in the health sector. At the same time, new vulnerabilities are frequently made public, requiring an appropriate cybersecurity strategy, including tracking the alerts of various manufacturers or suppliers, informing various national security agencies, or acquiring/collaborating with organisations to obtain CERT-like services on vulnerabilities actively exploited by attackers.

An increasingly relevant approach in vulnerability management is the integration of artificial intelligence (AI) solutions into existing solutions (AI-driven vulnerability management) by using machine learning algorithms to improve vulnerability detection, prioritisation and remediation processes (Wan, et al. 2024). Thus, AI solutions can analyse in real time large amounts of data, from system and network logs to threat intelligence feeds, to identify patterns that suggest possible security weaknesses in the infrastructure. Commercial vulnerability management platforms such as Qualys VMDR, Tenable.io, Rapid7 InsightVM, or Darktrace have integrated machine learning algorithms to correlate known vulnerabilities with their level of active exploitation in the real environment (Tod-Răileanu, et al. 2024). Artificial intelligence can also be used in vulnerability prediction, which predicts the likelihood of a newly discovered vulnerability being exploited, based on the historical behaviour of attackers and associated attack vectors.

The digitalisation of the health sector also requires the integration of specific technologies, systems and protocols, such as pharmacy management systems, ambulance and emergency services, and laboratory information systems. Among the most important are Electronic Health Records, which integrate patient histories using standards such as HL7 (Health Level 7) for the exchange of information between systems such as Radiology Information Systems and Laboratory Information Systems. Systems such as Picture Archiving and Communication Systems (PACS) are used to store and manage medical imaging, while the Digital Imaging and Communications in Medicine (DICOM) standard enables interoperability between imaging devices and storage systems. These technologies represent an additional attack surface to be considered by organisations in the medical sector, both for hospitals, clinics and for medical imaging centres, medical analysis laboratories, dental practices.

Vulnerabilities in medical devices

Modern medical devices such as heart monitors, ventilators and insulin pumps are increasingly integrated into the digital infrastructure of hospitals through the Internet of Medical Things (IoMT). This connectivity allows real-time monitoring of patients and automatic transmission of data to clinical information management systems, thereby improving the efficiency of healthcare. The devices communicate using standard protocols such as Wi-Fi and Bluetooth, as well as proprietary protocols developed by medical equipment manufacturers. This connectivity, while operationally beneficial, poses challenges in terms of cybersecurity, in particular in protecting the confidentiality, integrity and availability of patients' data.

To ensure secure transmissions, additional protection technologies such as VPNs and TLS/SSL encryption are also used over traditional network protocols such as TCP/IP, which allow communication between devices. These mechanisms reduce the risk of interception of sensitive information and protect against cyberattacks

targeting medical infrastructure. However, many IoMT devices remain vulnerable due to unsafe configurations, lack of software updates, or security standards that vary between different manufacturers.

A study of medical devices (Cynerio 2023) looked at the safety of medical devices in 14 NHS trusts, representing 6.4% of all NHS trusts, entities of the British health sector. These institutions were selected to reflect the diversity of hospitals in terms of size, number of beds and level of funding. The study used an anonymised analysis tool to identify the main risks, vulnerabilities and active threats associated with IoMT devices. The findings highlighted critical issues, including the possibility of exploiting unpatched vulnerabilities in more than 40 percent of devices, unsafe network configurations or the risk of unauthorised access. At the same time, more than 36.7% of devices would face reduced risks by implementing appropriate micro-segmentation at the network level.

The Human Factor in Cybersecurity

Information systems in healthcare facilities are susceptible to a number of vulnerabilities originating from the human factor. These weaknesses, while not correlated with common vulnerabilities and exposures or specific CVEs, are a critical vector in cyber risk assessment. The analysis of these vulnerabilities requires a contextual approach, given the workflows and human interactions in the medical field.

Attack vectors and human errors in the hospital context: One of the predominant attack vectors is phishing campaigns, where staff are misled by means of e-mails imitating legitimate sources. This manipulation results in compromising authentication data or installing malicious software. In parallel, poor credential management practices, such as using poorly configured passwords or reusing them across multiple platforms, facilitate unauthorised access.

Internal threats and social engineering: Internal threats from employees with malign intentions or grievances pose a significant risk, as they may abuse access privileges to exfiltrate sensitive data or disrupt operations. In addition, social engineering techniques, which manipulate staff to divulge confidential information or perform actions that compromise security, underline the importance of awareness and continuous training.

Inadequate data management and shortcomings in staff training: Improper handling of sensitive data, by accidentally transmitting patient information through unsecured channels or unintentionally exposing it, is another category of risk. Shortcomings in cybersecurity training programmes contribute to this vulnerability, with staff often not familiar with the latest security threats and practices.

Weaknesses in access control and non-compliance with security protocols: Poor user access management, manifested by failure to update access rights following changes in roles or leaving the organisation, creates entry points for attackers. Failure to comply with security protocols, such as ignoring software updates or bypassing virtual private networks (VPNs), additionally exposes systems to known vulnerabilities.
Risks associated with mobile devices and unintended disclosure: The loss or theft of mobile devices containing sensitive data poses a considerable risk of information exfiltration. Also, unintentional disclosure of data through mis transmission or leaving screens unattended are additional risks that can be mitigated by implementing a security-oriented organisational culture.

Perception of sector representatives on the level of cybersecurity

In recent years, in addition to the ransomware attacks that affected the activity of hospital units in Romania, organisations have been exposed to a variety of cyberattacks, highlighting an increasingly sophisticated threat landscape. One of the surveys conducted within the project with IT representatives and the management of 30 medical organizations in Romania generated data that provide clues on the level of preparedness of these organizations in the face of cyber threats, as well as on the perception of the subjects on the current state of cyber security in the sector.

According to responses collected from industry representatives, phishing and spear-phishing accounted for the largest share of reported incidents over the past three years, followed by Distributed Denial of Service (DDoS) attacks aimed at freezing IT infrastructures and brute force attacks used to compromise access credentials. Also, a significant category of threats was the distribution of malware and spyware, indicating a diversification of methods used by attackers. This hierarchy of incidents underlines the dynamic and adaptable nature of cyber threats as well as the need to implement multilateral security measures. In particular, the prevalence of phishing attacks justifies the need to consider human vulnerabilities as a vector of exploitation within cybersecurity systems.

Regarding the assessment and prioritisation of cyber vulnerabilities within organisations, participants provided varied answers on the existence of specific frameworks or methodologies used to determine the level of risk associated with each vulnerability. Of the 30 respondents, 12 said they did not have such a structured programme for managing vulnerabilities. However, around half of the participants use vulnerability scanning tools, intrusion detection systems (IDS) or other automated tools to identify risks and threats. These results point to a heterogeneous approach to cybersecurity in the sector, where, despite efforts to monitor threats,

a significant proportion of organisations are still not implementing a formalised vulnerability assessment and management process.

The low level of cybersecurity and the low capacity to manage incidents within organisations are attributed to a combination of technical, organisational and human factors. According to the data obtained, 28 out of 30 respondents indicated as main causes the use of obsolete or unsafe IT systems, the implementation of inadequate security controls and the limited resources allocated to the protection of the IT infrastructure. These factors not only increase the risk of compromising critical data and infrastructure but also make it difficult to implement proactive security measures.

A secondary but significant aspect identified in the analysis is the lack of cybersecurity awareness among employees, which contributes to additional vulnerabilities in the face of social engineering-based attacks such as phishing. These shortcomings reflect deeper systemic problems, in particular underfunding and underinvestment in cybersecurity infrastructure. In addition, they are amplified by human factors, including shortages of specialised staff, which limit the ability of organisations to effectively detect, prevent and respond to cyber incidents. The lack of a strategic commitment to developing a security-oriented organisational culture further aggravates risks, underlining the need for urgent measures to strengthen cyber resilience at institutional level.

Conclusions

Romania has made significant progress in digitalising the health sector, accelerated by the COVID-19 pandemic; the transformation has, however, increased cyber risks, exposing networks and patient data to threats. In this article, we highlighted the technical and non-technical vulnerabilities of the sector, obtained both from documentary research and questionnaires with representatives from the sector. The highlighted problems of the sector, from the use of obsolete software to the lack of cybersecurity-trained staff in both the public and private sectors, underline the need for stricter measures to protect health IT infrastructure against growing threats.

To protect critical health infrastructure and patient data, effective vulnerability management, software upgrades and IT infrastructure upgrades are needed. Given the different levels of cybersecurity maturity of the organisations in the system, the resilience of the health system requires a coherent national strategy based on investment in technology, cybersecurity training and effective risk management policies.

As technology advances, the integration of artificial intelligence could play a decisive role in proactively addressing cyber risks, both in the health sector and in other critical sectors. By automating processes to identify risks and threats and prioritise

vulnerabilities, AI-enabled solutions can greatly improve responsiveness and operational efficiency. Adopting a national strategy that includes such technologies could be an asset for Romania in protecting critical infrastructures and increasing cyber resilience at the national level.

References

Cisco Systems Inc. 2023. *Understanding the Phobos affiliate structure and activity.* https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/.

Cynerio. 2023. "The State of NHS Trust IoT Device Security 2023." https://www.cynerio.com/nhs-trusts-iot-security-report-cynerio-only.

DNSC. 2024. "Backmydata Ransomware (Alert)." https://www.dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf.

ENISA. 2023. "Enisa Threat Landscape: Health Sector." https://www.enisa.europa.eu/publications/health-threat-landscape.

___. 2024. "ENISA Threat Landscape 2024." doi:10.2824/0710888.

NIST. n.d. *CVSS – Vulnerability Metrics.* Accessed December 2024. https://nvd.nist.gov/vuln-metrics/cvss.

ProTV. 2023. *Spital din Botoșani, atacat de hackeri. Le-au criptat baza de date și cer 50.000 de dolari răscumpărare.* https://stirileprotv.ro/stiri/ilikeit/spital-din-botosani-atacat-de-hackeri-le-au-criptat-baza-de-date-si-cer-50-000-de-dolari-rascumparare.html.

RO-CCH. 2025a. *About RO=CCH.* https://rocch.ro/en/about-ro-cch.

___. 2025b. *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1).* RO-CCH - DIGITAL-2022-CYBER-02. https://rocch.ro/en/dissemination/deliverables/d2-1/download.

SecurityScorecard. n.d. *CVE Details.* Accessed December 2024. https://www.cvedetails.com/.

SRI. 2021. *Atac ransomware asupra Spitalului Clinic Witting din București.* https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html.

The MITRE Corporation. n.d. *CVE® Program Mission.* Accessed December 2024. https://www.cve.org/.

Tod-Răileanu, Gabriela, Ana-Maria Dincă, Sabina-Daniela Axinte, and Ioan C. Bacivarov. 2024. "Enhancing Vulnerability Management with Artificial Intelligence Algorithms." *International Conference on Cybersecurity and Cybercrime.* 96–101. doi:10.19107/CYBERCON.2024.13.

Wan, Shengye, Joshua Saxe, Craig Gomes, Sahana Chennabasappa, Avilash Rath, Kun Sun, and Xinda Wang. 2024. "Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia." *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S).* IEEE Computer Society. 80-87.

FINANCING INFORMATION

This research was partly made possible by the support of the RO-CCH project, which provided direct data on the management of cyber vulnerabilities in medical institutions in Romania through the *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1)*. The authors express their gratitude to health organisations and experts who contributed by participating in surveys and providing valuable insights.

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a grant for the implementation of the project 'Romanian Cyber Care Health - RO-CCH' under Grant Agreement No 101101522. The project is financed by the Funding Authority: CNECT.H – Digital Society, Trust, and Cybersecurity, under call DIGITAL-2022-CYBER-02-SUPPORTHEALTH.

DECLARATION ON CONFLICT OF INTERESTS

The authors declare that there are no potential conflicts of interest regarding the research, paternity and/or publication of this article.