Bridging the Maturity Gap: Adaptive Strategies for Advancing Cybersecurity in Romanian Healthcare Institutions

Claudia LASCATEU, Mihai CONSTANTINESCU
National Cyber Security Directorate
claudia.lascateu@dnsc.ro, mihai.constantinescu@dnsc.ro

Abstract: The current state of cybersecurity in many Romanian healthcare organisations remains at a "Defined" stage, which is characterized by documented and standardized processes. However, a significant maturity gap persists between these organisations and those that reach the "Managed" or "Optimised" stage - levels that involve the consistent monitoring and control, and the continuous improvement of cybersecurity practices. This progression is essential due to the sensitive nature of patient data and the increasing sophistication of cyber threats targeting the healthcare sector. This study explores how the Romanian healthcare institutions can transition from the "Defined" to the "Optimised" cybersecurity maturity level, and proposes adaptive strategies that integrate real-time threat intelligence, automated incident response mechanisms, and continuous training. The research hypothesis states that such adaptive strategies can significantly enhance the maturity transition process, offering a resilient defense against the evolving cyber threats. This hypothesis was tested through a mixed-methods approach, combining quantitative data from surveys and qualitative insights from expert interviews within the Romanian healthcare sector. Grounded in the findings outlined in the RO-CCH (Romanian Cyber Care Health) project's report on cybersecurity maturity, this paper provides a novel perspective, aligning the strategic importance of automation and continuous improvement with certain practical, actionable steps for improving the cybersecurity posture of Romanian healthcare institutions.

Keywords: cybersecurity maturity, Romanian healthcare institutions, adaptive strategies, automated incident response, threat intelligence, RO-CCH project.

INTRODUCTION

Cybersecurity in healthcare has become a critical issue in recent years due to the growing sophistication of cyberattacks and the increasing digitalization of medical records. Healthcare institutions face unique challenges in safeguarding sensitive patient information, ensuring the integrity of medical devices, and maintaining uninterrupted service delivery. Despite the importance of robust cybersecurity measures, many healthcare organisations remain in the „Defined" stage of cybersecurity maturity, as documented in the RO-CCH project report and survey findings. This stage is characterized by the existence of documented

https://doi.org/10.54851/v6i2y202401

procedures that are not consistently monitored or continuously improved.

The healthcare sector's cybersecurity challenges are compounded by limited budgets, inadequate training, and a lack of collaboration with external cybersecurity experts. Unlike sectors such as finance and energy, which feature more advanced cybersecurity maturity levels, healthcare organisations struggle with adopting real-time threat intelligence systems and automated incident response mechanisms. The financial sector, for instance, has made significant investments in Security Operations Centers (SOCs) and automated incident response systems to mitigate the risks of cyberattacks. Similarly, the energy sector has implemented stringent cybersecurity regulations to protect critical infrastructure.

This article proposes a phased approach to advancing cybersecurity maturity in Romanian healthcare institutions. By addressing foundational gaps - such as inconsistent training, limited external partnerships, and the slow adoption of automation - this roadmap aims to enable healthcare organisations to transition from a „Defined" to an „Optimised" stage. Drawing on comparative insights from more mature sectors and based on the findings of the RO-CCH report, this study outlines actionable strategies to enhance the cybersecurity posture of healthcare institutions. By adopting these adaptive strategies, healthcare institutions can better protect sensitive patient data, improve their incident response capabilities, and ensure compliance with regulatory requirements.

CHALLENGES IN ADVANCING CYBERSECURITY MATURITY IN HEALTHCARE: INSIGHTS FROM THE ROMANIAN CONTEXT

This section shall detail the current maturity levels of Romanian healthcare institutions, highlighting the challenges identified in both the survey and the maturity report. Key areas would include budget constraints, the lack of dedicated cybersecurity teams, and gaps in training and technical expertise. It would set the stage for why a shift from the „Defined" to the „Optimised" stage is necessary but challenging. Cybersecurity maturity in the healthcare sector has become increasingly critical due to the sensitive nature of patient data, the digital transformation of medical records, and the rising threat of cyberattacks targeting healthcare institutions. The cybersecurity maturity levels in Romanian healthcare, as outlined in the recent RO-CCH report, reveal a significant gap between institutions that have established basic cybersecurity protocols and those that have implemented advanced, continuously improving measures. This section explores the specific challenges faced by Romanian healthcare institutions in advancing their cybersecurity maturity, drawing comparisons with other critical sectors such as finance and energy, which also face significant cybersecurity challenges.

According to the RO-CCH survey data, many Romanian healthcare institutions remain at a „Defined" stage of cybersecurity maturity. This stage is characterized by the existence of documented and standardized processes but lacks the consistent measurement, monitoring, and control necessary to advance to higher levels of maturity like the „Managed" and „Optimised" stages. Key challenges highlighted in the survey include:

- **Budgetary Constraints:** Many healthcare institutions report insufficient funds allocated for cybersecurity initiatives, making it difficult to invest in advanced technologies like automated incident response systems or to hire specialized personnel.
- **Training Gaps:** The survey data reveals that cybersecurity training often occurs on an annual or biannual basis, which is insufficient for keeping pace with the rapidly evolving threat landscape. This results in a workforce that may be unprepared for sophisticated phishing attacks or ransomware threats.
- **Lack of External Collaboration:** A significant portion of healthcare institutions indicated a lack of collaboration with external cybersecurity experts or organisations, which limits their access to up-to-date threat intelligence and best practices.

To better understand the challenges in achieving cybersecurity maturity in healthcare, it is useful to compare these findings with cybersecurity practices in other sectors that face similar levels of cyber risk, such as finance and energy:

- **Financial Sector:**
    - According to a 2023 report of Accenture, over 70% of financial institutions globally have reached the „Managed" stage of cybersecurity maturity, meaning they have consistent monitoring and incident response processes in place. This contrasts sharply with the healthcare sector, where most institutions are still in the „Defined" stage.
    - Financial institutions often allocate a higher proportion of their IT budget to cybersecurity (typically around 10-15%) compared to healthcare institutions, where investment is often lower. This disparity highlights the critical role of budget allocation in achieving higher maturity levels.
    - The financial sector has also adopted real-time threat intelligence systems more readily, due to the direct impact of cyber incidents on their operations and customer trust. This proactive approach has been key to advancing their maturity.
- **Energy Sector:**
    - The energy sector, like the healthcare sector, manages critical infrastructure, but it has made more progress in cybersecurity maturity due to stringent regulatory requirements. A 2023 study by Deloitte found that 65% of energy companies in the EU had achieved the „Managed" or „Optimised" levels.
    - Energy companies benefit from industry-specific frameworks like the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards, which drive compliance and maturity. Such frameworks are less universally applied in the healthcare sector, leading to a higher variation in maturity levels among healthcare providers.
    - The energy sector has also invested heavily in continuous training, recognizing the role of human error in cyber incidents. This has helped to reduce the risk of breaches caused by phishing and social engineering - key challenges also noted in the healthcare survey.

The challenges faced by healthcare institutions in advancing their cybersecurity maturity have significant implications, both for this sector itself and for broader societal health and safety:

- **Increased Vulnerability to Cyberattacks:**
    - The lack of managed processes in many healthcare institutions means that they are more vulnerable to sophisticated cyberattacks such as ransomware, which can lock down critical systems and compromise patient data. The collected survey data indicates that many institutions do not update their cybersecurity tools and systems frequently enough to counter the emerging threats.
    - A 2024 report by the Ponemon Institute highlighted that the healthcare sector faced the highest average cost of a data breach among all industries, reaching $10.93 million per breach. This makes the impact of inadequate cybersecurity maturity not only a risk to patient safety but also a substantial financial burden.
- **Operational Disruptions and Service Delays:**
    - The inability to respond swiftly to cyber incidents can lead to significant disruptions in healthcare services, as seen in various high-profile ransomware attacks on hospitals worldwide. For example, the 2022 ransomware attack on Ireland's Health Service Executive (HSE) resulted in the cancellation of many critical patient services for weeks. Similar incidents could be devastating

for healthcare providers in Romania, particularly those with a limited level of cybersecurity maturity.
  - Disruptions to critical services can directly affect patient outcomes, especially in emergencies where timely access to digital medical records is crucial. The survey data suggests that many Romanian healthcare institutions lack the capacity to rapidly recover from such incidents.
- **Regulatory Risks and Compliance Issues:**
  - Healthcare providers are subject to stringent data protection regulations like the GDPR, which impose heavy fines for data breaches. A lack of robust cybersecurity practices can lead to non-compliance, resulting in legal liabilities and financial penalties.
  - In comparison with sectors like finance, where regulatory frameworks drive cybersecurity maturity, the healthcare sector in Romania faces challenges due to a less consistent enforcement of such frameworks and varying levels of awareness among institutions. The survey findings suggest that many healthcare providers do not conduct regular risk assessments, a key component for achieving compliance.

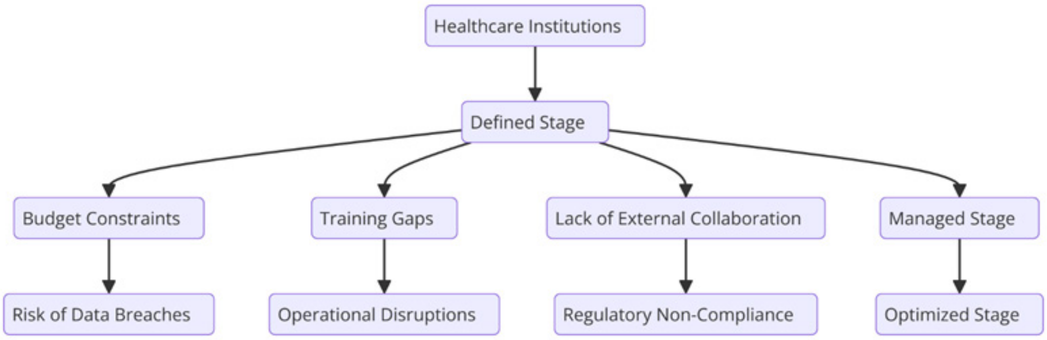

Figure 1. *The representation of the logical mind map regarding the defined stage of cybersecurity and the direct causes and effects on cybersecurity in the Romanian healthcare institutions*

The diagram highlights key challenges such as budgetary constraints, insufficient training, and limited external collaboration, which collectively hinder progress to higher maturity levels. It also illustrates the direct consequences of these issues, including increased vulnerability to cyber threats, operational disruptions, and regulatory non-compliance. This framework provides a clear depiction of the systemic barriers faced by healthcare institutions and sets the foundation for proposing targeted solutions in subsequent sections of the article.

In conclusion, the RO-CCH report highlights that many healthcare institutions remain at a „Defined" stage of maturity, struggling to move towards a more „Managed" or „Optimised" status. A significant challenge also noted is the limited frequency of updates and insufficient training, as seen in the survey responses according to which many institutions only conduct updates and training on a quarterly basis. While the study hypothesis suggests that integrating real-time threat intelligence and automated incident responses can elevate cybersecurity maturity levels, the survey data points to the underlying issues such as budget constraints and a lack of consistent management commitment. These factors could hinder the adoption of real-time and automated solutions, suggesting that adaptive strategies alone may not be sufficient without addressing organisational and financial barriers first.

The comparison between the cybersecurity maturity level of the healthcare sector and of other critical industries like finance and energy highlights both the challenges and opportunities for improvement. While the healthcare sector lags behind in key areas such as real-time threat intelligence, budget allocation, and continuous training, these are areas where targeted investments and strategic improvements could yield significant benefits. Addressing the maturity gap is not only a technical challenge but also one related to organisational change, requiring a shift in priorities and a stronger commitment to cybersecurity at all levels of management. By learning from the practices of more mature sectors, healthcare institutions can develop a roadmap to enhance their cybersecurity posture, ultimately protecting patient data and ensuring the resilience of essential health services.

EVALUATING THE ROLE OF ADAPTIVE STRATEGIES: REAL-TIME INTELLIGENCE AND AUTOMATION IN HEALTHCARE CYBERSECURITY

This section critically examined the proposed adaptive strategies (real-time threat intelligence, automated incident response, and continuous training). It analysed how these strategies align with the specific needs and readiness of healthcare institutions, using data from the survey to discuss practical implementation barriers. It also explored scenarios where these strategies have succeeded or failed due to contextual factors like resource availability and management commitment.

The survey data indicates that many institutions face challenges in collaborating with external experts and implementing new technologies. For example, several respondents mentioned a lack of collaboration with external cybersecurity experts, which can be critical for implementing sophisticated tools like SIEM or EDR.

Real-Time Threat Intelligence: Essential Yet Challenging for Healthcare

The RO-CCH report and survey data indicate that most Romanian healthcare institutions have not fully implemented real-time threat intelligence systems. The majority of them rely on periodic updates and basic alert systems rather than continuous monitoring. Only a few institutions have invested in Security Information and Event Management (SIEM) tools or similar technologies, which can correlate real-time data to identify potential threats.

By contrast, the financial sector has made significant strides in adopting real-time threat intelligence. According to a 2023 Accenture report, over 80% of global financial institutions utilize SIEM systems for real-time monitoring, and 60% have dedicated Security Operations Centers (SOCs). This approach has enabled a rapid threat detection and mitigation, which is crucial in a sector where downtime and breaches can have immediate financial consequences.

The lack of real-time threat intelligence in healthcare creates vulnerabilities, making institutions slower to respond to emerging threats like ransomware and phishing. This delay increases the likelihood of data breaches, with potential costs running into millions. For instance, the Ponemon Institute's 2024 report found that healthcare data breaches cost on average $10.93 million per incident. Real-time threat intelligence could reduce detection and response times, potentially mitigating these costs. However, the initial investment and need for skilled personnel remain significant barriers, as identified in the survey findings.

Automated Incident Response: A Path to a Faster Recovery but Resource Intensive

The survey data reveals that only a minority of Romanian healthcare institutions have adopted automated incident response mechanisms. Most rely on manual processes, which are often slow and inefficient. The RO-CCH report highlights that many institutions lack the technical capacity and expertise to deploy tools like Endpoint Detection and Response (EDR), a critical component for automation.

By comparison, the energy sector has embraced automation more robustly. A 2023 Deloitte study reported that 65% of energy companies in the EU have integrated automated incident response as a part of their cybersecurity frameworks. This integration is driven by the critical nature of energy infrastructure and strict regulatory requirements, such as the NIS2 directive, which mandates rapid incident response capabilities.

The limited adoption of automated incident response in healthcare contributes to an extended downtime during cyber incidents. For example, healthcare providers affected by ransomware attacks have faced service disruptions lasting several weeks. The reliance on manual processes means that healthcare institutions struggle to restore operations quickly, which impacts patient care and safety. Automation could drastically reduce recovery times, but it requires investment in technology and training. Without addressing these resource gaps, the healthcare sector may continue to lag behind other critical industries with regard to incident response readiness.

Continuous Training: A Critical Component with Inconsistent Implementation

Training and awareness remain key priorities for improving cybersecurity maturity in healthcare, yet its implementation is inconsistent. The survey indicates that most Romanian healthcare institutions conduct training annually or biannually, few of them opting for more frequent sessions like quarterly updates. The RO-CCH report emphasizes the need for continuous training, especially as phishing and social engineering remain common attack vectors.

The financial sector has a more rigorous approach to training. A study by IBM in 2023 noted that over 75% of financial institutions conduct quarterly training sessions for all employees, supplemented by monthly phishing simulations. This continuous engagement helps maintain a high level of awareness among the staff, reducing the risk of successful phishing attempts.

The inconsistent implementation of training in healthcare leaves gaps in staff preparedness, making institutions more susceptible to social engineering attacks. As seen in the RO-CCH survey, a lack of regular training can lead to a workforce that is less vigilant against the emerging threats. This gap contrasts sharply with the situation in the financial sector, where ongoing training has become standard. Addressing this issue in healthcare could significantly reduce the risk of data breaches caused by human error, but it requires commitment to resource allocation and a shift in organisational culture towards continuous learning.

In conclusion, the study hypothesis assumes that healthcare institutions are ready for a technological shift, but the survey data reveals a gap in technical expertise and external support. Without foundational investments in staff training and external partnerships, the deployment of advanced, automated systems might be impractical. The analysis reveals that while adaptive strategies like real-time threat intelligence, automated response, and continuous training hold great potential for enhancing cybersecurity maturity in the healthcare sector, their successful implementation faces several hurdles. Unlike the financial and energy sectors, where the adoption of these strategies is more advanced, healthcare institutions struggle with limited budgets, insufficient expertise, and organisational inertia. Bridging this gap will require a phased approach, starting with foundational improvements in training and resource allocation before more advanced technologies can be adopted. Addressing these barriers is essential for improving the resilience of healthcare institutions against the increasingly sophisticated cyber threats.

BRIDGING THE GAP: A PHASED APPROACH TO IMPLEMENTING ADAPTIVE CYBERSECURITY SOLUTIONS

Drawing on the survey findings, the RO-CCH maturity report, and comparative data from other sectors, this section outlines a phased approach to enhancing cybersecurity maturity in Romanian healthcare institutions. By starting with foundational improvements such as increased training, building partnerships with cybersecurity experts, and gradually introducing automation, this roadmap aims to bridge the significant gap between the „Defined" and „Optimised" cybersecurity maturity stages. This section will also include a comparative analysis involving implementation strategies in other sectors, such as finance and energy, which offer valuable lessons for healthcare.

Foundational Improvements: Focus on Training and Awareness

Survey Findings:

A majority of healthcare institutions in Romania are still in the „Defined" stage of cybersecurity maturity, where documented and standardized processes exist but are not regularly updated or improved. The survey revealed that many healthcare institutions conduct cybersecurity training only annually or biannually, leaving gaps in staff preparedness for phishing attacks and other social engineering threats.

Comparative Sector Analysis:

In the financial sector, continuous training is a cornerstone of cybersecurity. A 2023 IBM report found that over 75% of financial institutions conduct quarterly training and phishing simulations. This approach has led to a significant reduction in successful phishing attempts.

The energy sector has also adopted robust training programs as part of its cybersecurity strategy, with many institutions conducting monthly or quarterly sessions to mitigate the risk of human error during cyber incidents.

Recommendations for the Healthcare sector:

- **Increase Training Frequency:** Romanian healthcare institutions should move from annual to quarterly training sessions, following the lead of more mature sectors like finance and energy. Regular phishing simulations and targeted training can significantly enhance staff awareness and reduce vulnerability to social engineering attacks.
- **Tailored Training Modules:** Romanian healthcare institutions should implement adaptive training that targets different levels of their staff. For instance, clinical staff could receive tailored training focused on protecting patient data, while IT staff could receive more technical training on mitigating ransomware and DDoS attacks.

Impact Analysis:

An enhanced training frequency and targeted awareness campaigns are likely to improve the cybersecurity maturity of healthcare institutions by addressing one of the primary vulnerabilities - human error. A more vigilant workforce can lead to a reduction in successful phishing attacks, which currently account for a significant portion of the cyber incidents in this sector.

Building Strategic Partnerships: Leveraging External Cybersecurity Expertise

Survey Findings:

Many healthcare institutions in Romania reported limited collaboration with external cybersecurity experts. This lack of access to up-to-date threat intelligence and advanced cybersecurity solutions has left these institutions vulnerable to sophisticated attacks.

Comparative Sector Analysis:

In the energy sector, collaboration with cybersecurity experts is often mandated by regulatory frameworks such as the NIS2 Directive, which ensures that institutions have access to real-time threat intelligence and expert support during incidents. The financial sector similarly prioritizes partnerships with cybersecurity firms, many of which offer Security Operations Center (SOC) services that provide round-the-clock monitoring and incident response.

Recommendations for the Healthcare sector:

- **Engage External Experts:** Healthcare institutions should establish partnerships with cybersecurity providers who can offer managed services, such as Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools. This will allow them to benefit from the expertise and resources of professionals who specialize in detecting and mitigating complex cyber threats.

- **Collaborate on Threat Intelligence:** Healthcare institutions should join threat intelligence sharing platforms, where they can receive real-time updates on the emerging cyber threats. This proactive approach, already adopted by sectors such as finance, could significantly improve incident response times and threat mitigation efforts.

Impact Analysis: By engaging with external experts, healthcare institutions can bridge the technical expertise gap and implement more sophisticated cybersecurity measures. This will also reduce the burden on internal IT staff, who may lack the skills to manage advanced systems like SIEM and EDR. In the long term, collaboration will improve resilience against cyberattacks, particularly ransomware and data breaches, which are becoming increasingly common in the healthcare sector.

Gradual Introduction of Automation: Enhancing Incident Response

Survey Findings:

The RO-CCH maturity report highlights that most healthcare institutions in Romania rely on manual incident response processes, which are often slow and ineffective. Automated incident response systems, such as EDR and automated phishing filters are rarely used due to budgetary constraints and technical limitations.

Comparative Sector Analysis:

The financial sector has heavily invested in automation to reduce incident response times. According to a 2023 Accenture report, over 60% of financial institutions have deployed automated incident response systems. These systems significantly reduce the time it takes to detect, analyse, and respond to threats, thus minimizing operational disruptions.

In the energy sector, the implementation of automated response mechanisms, mandated by regulations such as the NIS2 Directive, has improved the sector's ability to swiftly contain threats and restore normal operations.

Recommendations for the Healthcare sector:

- **Phased Implementation of Automation:** Given the budget constraints reported by many healthcare institutions, a phased approach is recommended. Healthcare institutions should start by automating high-risk areas, such as email security and phishing detection. More advanced solutions like EDR and SIEM should be gradually introduced as budgets allow.
- **Pilot Programs for Automation:** Healthcare institutions could start with small-scale pilot programs to test the efficacy of automated systems. These programs could focus on areas where automation could have the most immediate impact, such as detecting ransomware or managing network traffic anomalies.

Impact Analysis:

Automation will enhance the speed and efficiency of cybersecurity responses in healthcare, reducing the time for detecting and responding to threats. This will be especially critical in minimizing the impact of ransomware attacks, which currently disrupt healthcare services for extended periods. As automation is phased in, healthcare institutions will experience fewer disruptions, better data protection, and an improved regulatory compliance.

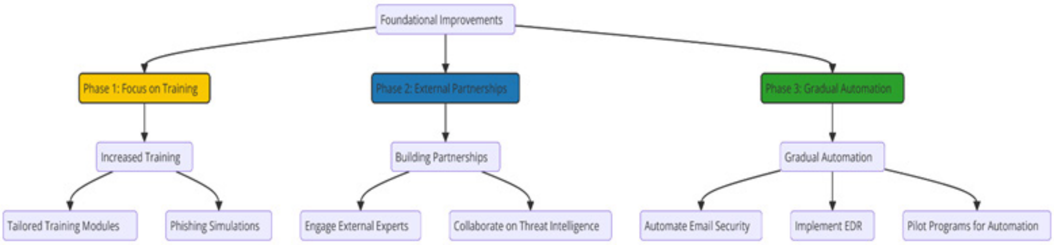
Foundational Improvements
Phase 1: Focus on Training
Phase 2: External Partnerships
Phase 3: Gradual Automation
Increased Training
Building Partnerships
Gradual Automation
Tailored Training Modules
Phishing Simulations
Engage External Experts
Collaborate on Threat Intelligence
Automate Email Security
Implement EDR
Pilot Programs for Automation

Figure 1. *The representation of the logical mind map regarding the defined stage of cybersecurity and the direct causes and effects on cybersecurity in the Romanian healthcare institutions*

The diagram outlines progressive steps starting with foundational improvements, such as increased training frequency and enhanced collaboration with cybersecurity experts, followed by the gradual introduction of automation in high-risk areas. It also illustrates the short-term impacts of these measures on organizational maturity, emphasizing how targeted investments and strategic initiatives can facilitate the transition from the „Defined" stage to higher maturity levels. This visual serves as a roadmap for implementing adaptive cybersecurity solutions effectively.

By adopting a phased approach, Romanian healthcare institutions can bridge the gap between their current „Defined" stage of cybersecurity maturity and the more advanced „Managed" or „Optimised" stages. Starting with foundational improvements in training, followed by building partnerships with external cybersecurity experts, and gradually introducing automation, these institutions can enhance their resilience against cyber threats. Comparative insights related to the financial and energy sectors demonstrate that targeted investments in these areas can yield significant improvements in cybersecurity posture. In the long term, these changes would not only protect sensitive patient data but also ensure the continuity and safety of critical healthcare services.

The research presented in this article highlights the significant challenges and opportunities for improving the cybersecurity maturity of Romanian healthcare institutions. As revealed by the RO-CCH project and survey findings, many healthcare organisations remain in the „Defined" stage of cybersecurity maturity, struggling to advance towards the more resilient „Managed" and „Optimised" stages. These institutions face budgetary constraints, inconsistent training practices, and limited access to external expertise, all of which hinder the adoption of advanced cybersecurity strategies such as real-time threat intelligence, automated incident response, and continuous training.

Through a phased approach, this article proposes practical steps for bridging this maturity gap. Foundational improvements, such as increasing the frequency and scope of cybersecurity training, building strategic partnerships with cybersecurity experts, and gradually introducing automation, are essential for enhancing the overall cybersecurity posture. Comparative insights from more mature sectors like finance and energy demonstrate that targeted investments in these areas can lead to significant improvements regarding both threat detection and incident response capabilities.

The proposed roadmap aims to equip healthcare institutions with the necessary tools and strategies to not only protect sensitive patient data but also ensure the continuity of critical healthcare services in the face of increasingly sophisticated cyber threats. By adopting a phased, strategic approach, Romanian healthcare institutions can elevate their cybersecurity maturity, which would ultimately lead to more robust defense mechanisms and a better regulatory compliance.

CONCLUSION

This study contributes to the discourse on advancing cybersecurity maturity in critical sectors by contextualizing the specific challenges and opportunities within the Romanian healthcare system. By adopting a phased and strategic approach informed by best practices from more mature industries, healthcare institutions can mitigate vulnerabilities, safeguard sensitive data, and ensure the resilience of essential services in an increasingly complex threat landscape. This research underscores the importance of sustained investment in cybersecurity as a foundational element of modern healthcare infrastructure.

ACKNOWLEDGEMENT
This research was made possible partially through the support of the RO-CCH project, which provided valuable direct data on the current cybersecurity maturity level of the Romanian healthcare institutions. The authors would like to extend their gratitude to all the healthcare organisations and experts who participated in the surveys and shared their insights.

ENDNOTES
The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of "Romanian Cyber Care Health - RO-CCH" project, under the grant agreement no. 101101522. The project is financed through granting authority: CNECT.H – Digital Society, Trust, and Cybersecurity, under the call DIGITAL-2022-CYBER-02-SUPPORTHEALTH topics, type of action: Digital SME Support Actions.
Cyber organisational maturity and operational models for healthcare and health institutions (D1.2) of "Romanian Cyber Care Health - RO-CCH" project.

REFERENCE LIST

Dal Cin, P., Fox, J., Sidhu, H. & Nunn-Price, J. (2023a) *How cybersecurity boosts enterprise reinvention to drive business resilience - State of Cybersecurity Resilience 2023*. Available at: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf [Accessed 20th October 2024].

Dal Cin, P., Fox, J., Sidhu, H. & Nunn-Price, J. (2023b) *State of Cybersecurity Resilience 2023 - How cybersecurity boosts enterprise reinvention to drive business resilience*. 10-minute read. Available at: https://www.accenture.com/us-en/insights/security/state-cybersecurity [Accessed 24th October 2024].

Deloitte. (n.d.) Five in 5: *Cybersecurity in the energy sector - Energy cybersecurity risks and mitigation strategies*. https://www2.deloitte.com/us/en/pages/consulting/articles/cybersecurity-energy-sector.html [Accessed 22nd October 2024].

Deloitte. (2023) 2023 *Global Future of Cyber Survey*. https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf [Accessed 21st October 2024].

Deloitte. (2024) *Cyber in Energy - An escalating risk to critical infrastructure technology and processes*. https://www.deloitte.com/au/en/Industries/power-utilities-renewables/analysis/cyber-in-energy-escalating-risk-critical-infrastructure-technology-processes.html [Accessed 22nd October 2024].

Gobi, S. (2024) *Banking Cybersecurity Trends and Strategies: Safeguarding Data from Cyber Threats and Piracy in 2024 and Beyond* [LinkedIn], 13 March. Available from: https://www.linkedin.com/pulse/banking-cybersecurity-trends-strategies-safeguarding-data-gobi-s-lhjec/ [Accessed 20th October 2024].

IBM. (2024) *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach [Accessed 23rd October 2024].

Ige, T. O., Frimpong, A. A. & Akinbobola, B. A. (2024) Mitigating Cybersecurity Threats in the Healthcare Sector: An Analysis of Challenges and Solutions in the USA. *Journal of Energy Technologies and Policy.* 14(2), 66-76. doi: 7176/JETP/14-2-05.

Möller, D. P. F. (2023) Cybersecurity Maturity Models and SWOT Analysis. In: *Guide to Cybersecurity in Digital Transformation. (Advances in Information Security, vol. 103)*. Cham, Switzerland, Springer.

North American Electric Reliability Corporation (NERC). (n.d.) Standards. https://www.nerc.com/pa/Stand/Pages/Default.aspx [Accessed 22nd October 2024].

Office of Information Security. (2022) *HHS Cybersecurity Program, Leadership for IT Security & Privacy across HHS, Lessons Learned from the HSE Cyber Attack.* https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf [Accessed 23rd October 2024].

Pal, P. (2022) The adoption of waves of digital technology as antecedents of digital transformation by financial services institutions. *Journal of Digital Banking.* 7(1), 70-91. doi: 10.69554/QHFT9370.

Ponemon Institute. (2024) *The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care.* https://assets.turtl.co/customer-assets/tenant%3Dteam/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report-2024%20(1).pdf [Accessed 22nd October 2024].

Romanian National Cyber Security Directorate (DNSC). (n.d.) Romanian Cyber Care Health - RO-CCH https://dnsc.ro/pages/proiect-ro-cch [Accessed 20th October 2024].

Ronquillo, J. G., Winterholler, J.E., Cwikla, K., Szymanski, R.& Levy, C. (2018) Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open.* 1(1), 15-19. doi: 10.1093/jamiaopen/ooy019.