Journal of Engineering Science *Vol. XXXII, no. 1 (2025), pp. 18 - 31*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2025.32(1).02
UDC 004.056:004.8

REDUCING CYBER RISK THROUGH A HUMAN–CENTRED APPROACH

Ludmila Peca *, ORCID: 0000-0002-4394-2933,
Dinu Ţurcanu, ORCID: 0000-0001-5540-4246

Technical University of Moldova, National Institute of Innovations in Cybersecurity,
168 Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Ludmila Peca, *ludmila.peca@isa.utm.md*

Received: 12. 22. 2024
Accepted: 01. 29. 2025

Abstract. This paper investigates the complex challenges professionals face in managing cyber risks and implementing human risk management programs. Emphasizing the crucial role of human behavior in effectively mitigating cyber risks, the paper highlights the transformative impact of utilizing the „Golden Circle" methodology. This human-centered methodology initiates discussions with the question „WHY", articulating the fundamental purpose of human risk management and promoting an „inside-out" approach, starting with employee motivation and engagement. This approach ensures the sustainability of human risk management practices by fostering a sense of responsibility and belief in the mission. Furthermore, the integration of Artificial Intelligence (AI) is explored to enhance human risk management, with AI techniques such as machine learning analyzing behavioral patterns to predict potential risks and automate responses. However, the paper also addresses the drawbacks of AI, including sophisticated phishing attacks and deepfakes exploiting human vulnerabilities. Combining AI with the „Golden Circle" allows organizations to identify *why* employees are susceptible to attacks and *how* to tailor training, achieving a more robust and proactive risk management strategy. The paper offers tips and recommendations for evolving and sustaining this integrated methodology over time, ensuring its continued effectiveness in the dynamic cybersecurity landscape.

Keywords: *artificial intelligence, cybersecurity, „Golden Circle" method, security culture, educational programs, risk prediction.*

Rezumat. Această lucrare analizează provocările complexe cu care se confruntă profesioniștii în gestionarea riscurilor cibernetice și implementarea programelor de gestionare a riscurilor umane. Subliniind rolul crucial al comportamentului uman în atenuarea eficientă a riscurilor cibernetice, lucrarea evidențiază impactul transformator al utilizării metodologiei „Cercului de Aur". Această metodologie centrată pe om inițiază discuții cu întrebarea „DE CE", articulând scopul fundamental al gestionării riscurilor umane și promovând o abordare „din interior spre exterior", începând cu motivarea și implicarea angajaților. Prin cultivarea unui sentiment de responsabilitate și credință în misiune, această abordare asigură sustenabilitatea practicilor de gestionare a riscurilor umane. Mai mult, integrarea Inteligenței Artificiale (IA) este explorată pentru a îmbunătăți gestionarea riscurilor umane, cu tehnici de IA, cum ar fi

învățarea automată, care analizează modelele de comportament pentru a prezice potențialele riscuri și a automatiza răspunsurile. Cu toate acestea, lucrarea abordează, de asemenea, dezavantajele IA, inclusiv atacurile sofisticate de phishing și deepfakes care exploatează vulnerabilitățile umane. Combinarea IA cu „Cercul de Aur" permite organizațiilor să identifice *de ce* angajații sunt susceptibili la atacuri și *cum* să adapteze instruirea, realizând o strategie de gestionare a riscurilor mai robustă și proactivă. Lucrarea oferă sfaturi și recomandări pentru evoluția și susținerea acestei metodologii integrate de-a lungul timpului, asigurând eficacitatea sa continuă în peisajul dinamic al securității cibernetice.

Cuvinte cheie: *inteligență artificială, securitate cibernetică, metoda „Golden Circle", cultură de securitate, programe educaționale, predicția riscurilor.*

1. Introduction

In an era where cyber threats are becoming increasingly sophisticated and widespread, cyber risk management has evolved beyond the mere implementation of technological solutions. As organizations face ever more complex challenges, it is crucial to recognize the human factor's pivotal role in ensuring security. Cyber risks are no longer just a matter of technology but also human behavior and organizational culture. In this context, a people-centered approach to risk management becomes vital for long-term success.

In a digitalized era, the increasing dependence on the internet and global infrastructure exposes organizations to significant risks, including data theft, fraud, DDoS attacks, and the compromise of critical infrastructures. According to recent studies, attackers are employing increasingly sophisticated techniques such as social engineering, supply chain attacks, and zero-day exploits [1]. This underscores the necessity of integrating human-centered risk management strategies with technological advancements to effectively mitigate cyber threats.

2. A people-centered approach to risk management

Effective cyber risk management requires an approach that focuses on human behavior. Such an approach acknowledges that technology cannot provide a complete cybersecurity solution, no matter how advanced. The human factor, often the most vulnerable element in an organization, can also be the most powerful defense when properly engaged in the security strategy.

A clear example that demonstrates the impact of the human factor on cybersecurity is the attack on Colonial Pipeline fig. 1, where the compromise of a VPN account without multifactor authentication led to a major ransomware attack. This incident disrupted fuel supply across the U.S., highlighting the need for improved human risk management and the use of methods such as the 'Golden Circle' to enhance employee awareness.

For the authors of this article, the topic is particularly relevant as they are in the process of forming the team for the National Institute of Innovations in Cybersecurity „CYBERCOR". At this critical stage, integrating a people-centered approach is essential to ensure that the team not only adopts the best security practices but also understands the importance of human behavior in protecting the organization against cyber threats. By forming a team that is aware of the significance of the human factor and capable of implementing security strategies tailored to this reality, the National Institute of Innovations in Cybersecurity „CYBERCOR" aims to become an innovative leader in the field of cybersecurity.

Figure 1. Distribution and financial impact of insider threats [1].

To further strengthen this approach, aligning with established security standards is crucial. One such reference model for incident management is **ISO/IEC 27035:2023** [2], which provides a structured framework for identifying and responding to security incidents. By integrating this standard with the **Golden Circle methodology** [3], organizations can develop a more effective strategy for managing human-related cybersecurity risks [4]. This ensures not only a reactive but also a proactive approach to handling security threats.

To effectively address these challenges, it is essential to identify common human vulnerabilities in cybersecurity and explore how AI-driven solutions can mitigate these risks. Table 1 provides an overview of key human-related security weaknesses and the corresponding AI-based solutions that can enhance cybersecurity resilience.

Table 1

Addressing human vulnerabilities in Cybersecurity with AI solutions

Human vulnerability	Impact	AI solution proposed
Lack of multifactor authentication	Ransomware attacks and data breaches	AI-driven contextual authentication
Phishing and social engineering	Data leaks, financial fraud	AI-based anomaly detection in emails
Unauthorized access	Extraction of critical data	AI-powered access monitoring
Misconfiguration errors	Exploitable security vulnerabilities	AI-assisted configuration validation

In addition to addressing human vulnerabilities through AI-driven solutions, organizations must implement a structured incident response process to mitigate security risks effectively. The **Incident Handling Lifecycle** provides a systematic approach to managing cybersecurity incidents, ensuring a rapid and coordinated response to potential threats.

The **Incident Handling Lifecycle** consists of several key phases, each contributing to the containment, eradication, and prevention of cyber threats:

- **Detection & Identification**. Identifying potential security incidents through monitoring, anomaly detection, and user reports.
- **Triage & Prioritization**. Assessing the severity and impact of the incident to allocate resources effectively.

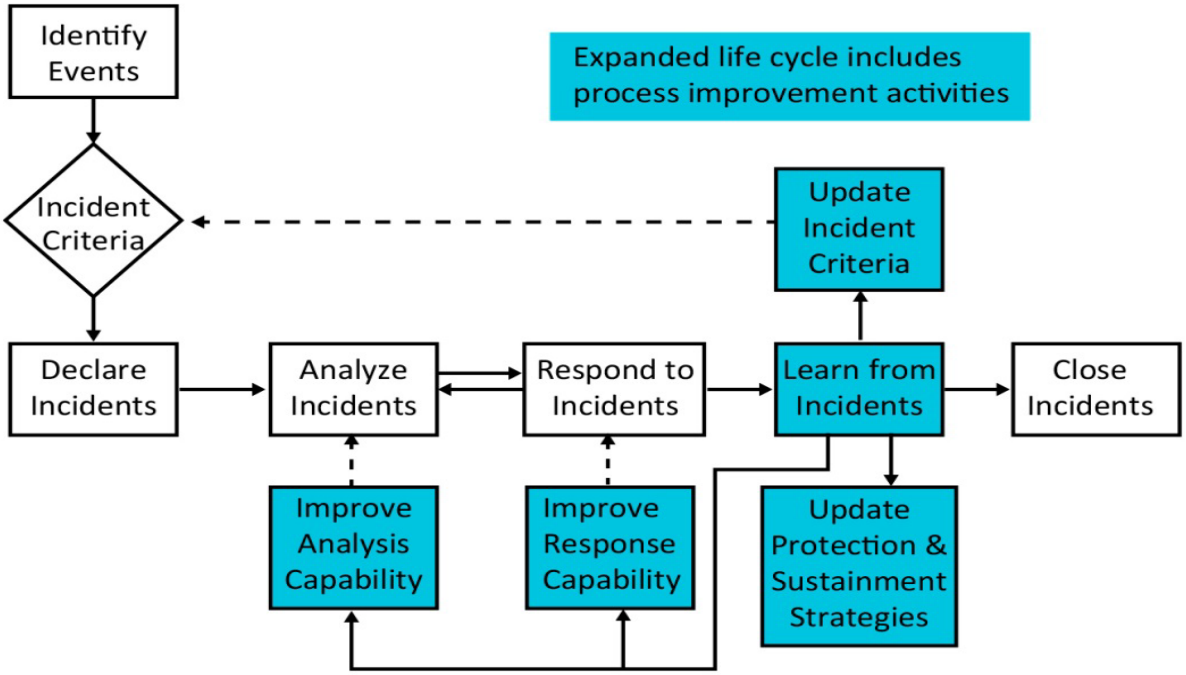

Figure 2. Expanded incident handling Lifecycle including process improvement activities [5].

- **Containment**. Implementing immediate measures to prevent further damage, such as isolating affected systems.
- **Eradication & Recovery**. Removing the threat, restoring affected systems, and ensuring no residual vulnerabilities remain.
- **Post-Incident Analysis**. Conducting a thorough review of the incident to improve future responses and prevent recurrence.

By integrating the **Incident Handling Lifecycle** with AI-driven security enhancements and internationally recognized standards such as **ISO/IEC 27035:2023**, organizations can build a more resilient cybersecurity framework, capable of both proactive risk management and efficient incident response.

3. The „Golden Circle" method and the importance of starting with „WHY"

A powerful example of a people-centered approach is the „Golden Circle" method proposed by Simon Sinek [6]. This method begins with the question „WHY?" - Why is cybersecurity important, and why must risk be managed in a specific way? Starting with this fundamental question, organizations can clearly articulate the purpose and significance of their risk management programs, helping to foster a sense of responsibility and engagement among all participants.

Communicating „from the inside out", beginning with „WHY", allows leaders to build a shared understanding and motivate employees to adopt behaviors that support security. Instead of viewing security requirements as additional tasks, employees understand the context and importance of their actions, leading to deeper engagement and proactive behavior.

A remarkable example of successful implementation of the „Golden Circle" methodology can be seen in a complex organization operating with multiple business units and diverse organizational cultures. In this case, leaders began by clarifying the „WHY" - the fundamental purpose of the cybersecurity program: protecting the integrity and operational

continuity in an increasingly threatening digital environment. This clarity of purpose enabled leaders to effectively communicate the importance of cybersecurity not just as a technical requirement but as an essential pillar for the long-term success and sustainability of the organization.

By focusing on „WHY", leaders were able to secure the commitment and active participation of employees, even in the face of significant challenges such as rapidly changing cyber threat landscapes and the integration of new processes into diverse organizational cultures. This commitment was crucial for the organization's continuous adaptation to emerging threats, ensuring not only compliance with security standards but also robust cyber resilience capable of meeting future challenges.

The people-centered approach not only improved compliance and adherence to security measures but also transformed the organizational culture, placing cybersecurity at the core of the organization's daily values and practices. This cultural shift was made possible only by recognizing and valuing the essential role of human behavior in risk management.

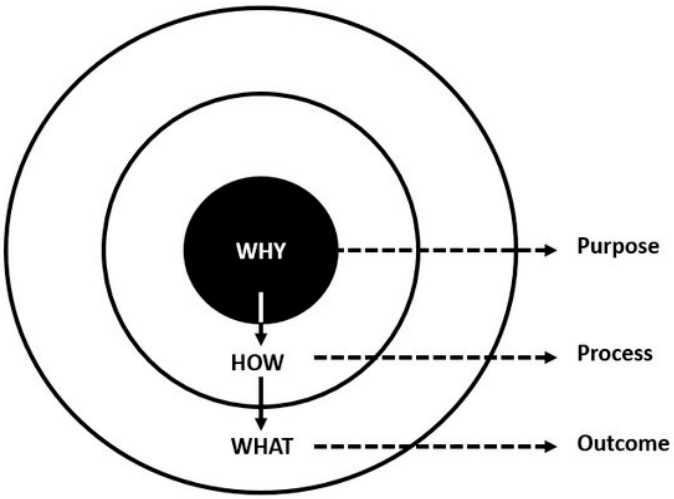

Figure 3. The „Start with Why" Golden Circle Model [6].

While the **Golden Circle** methodology emphasizes the **human factor** in cybersecurity, ensuring that employees and stakeholders understand and commit to security principles, it is equally important to leverage technological advancements to enhance risk management. As cyber threats evolve at an unprecedented rate, organizations must adopt **proactive, AI-driven security solutions** that complement human awareness and decision-making. **Artificial Intelligence** plays a crucial role in identifying threats, predicting vulnerabilities, and automating security processes, reducing the burden on human operators while improving overall cyber resilience.

4. Integrating artificial intelligence into risk management

As the cyber threat landscape continues to evolve, organizations face the need to adopt advanced technologies that allow them to stay one step ahead of attackers. AI has proven to be an essential ally in this regard, offering new ways of analyzing and predicting risks that are inaccessible through traditional methods.The use of AI in risk analysis and prediction is crucial in the current discussion, highlighting AI's ability to significantly revolutionize the ways organizations identify and manage cyber threats.

According to the definition provided by Stuart Russell and Peter Norvig, *„AI is the study of agents that receive percepts from the environment and perform actions. Each such agent*

implements a function that maps percept sequences to actions, and it is presumed that these actions are selected in such a way as to maximize some performance measure, given the evidence provided by the percept sequence. AI aims to develop machines and programs that can perform tasks considered intelligent if done by humans, using techniques such as machine learning, reasoning, and adaptation to improve performance based on experience" [7].

AI can be integrated into cybersecurity programs to enhance risk management through several methods:

Advanced behavioral analysis. AI, through the use of deep learning techniques, can analyze large volumes of data in real time to identify patterns and anomalies in user behavior. *Deep learning* is a subset of machine learning that utilizes artificial neural networks to learn from complex and unstructured data. This allows for the early detection of potential risks, such as unusual activities that might indicate an ongoing cyber attack. For example, AI can learn to recognize deviant behaviors that may signal a security breach, giving organizations time to respond before damage is done [8].

Risk prediction. By utilizing advanced machine learning techniques, AI can anticipate cyber threats, providing organizations with a proactive perspective on potential risks [9]. These techniques are based on analyzing historical data and observed behaviors, enabling AI to identify patterns that may predict attacks or security breaches before they materialize. By anticipating these threats, AI allows organizations to implement protective measures in advance, thereby reducing not only the risk of cyber attacks but also the resources and time required to respond to these incidents. This significantly improves overall security and operational efficiency.

Automating responses. AI plays a crucial role in automating responses to cyber attacks, allowing organizations to react quickly and efficiently to threats [10]. Using advanced algorithms, AI can autonomously detect and respond to incidents, such as isolating a compromised device to prevent the spread of an attack or blocking suspicious connections. Automation not only speeds up response times but also reduces the risk of human error, thereby helping to maintain operational continuity and minimize the impact of a cyber attack.

However, integrating AI into risk management is not without its challenges and risks. If not properly managed, AI technologies can introduce new vulnerabilities:

a. More sophisticated phishing attacks. AI can be used by attackers to create highly convincing phishing attacks that exploit personal data and human behaviors to deceive users. These attacks can be tailored to the victim's profile, making them much harder to detect [11].

b. Deepfakes and social engineering. *Deepfakes* are falsified audio or video materials created using advanced artificial intelligence techniques, particularly neural networks and deep learning. These can make it appear as if a person is saying or doing things they never actually did. AI can be used to generate such deepfakes that look extremely authentic, making them almost impossible to distinguish from real materials. These can be used to manipulate employees or mislead decision-makers, creating new attack vectors within organizations. Due to their realistic nature, deepfakes are difficult to combat through traditional security measures, requiring advanced strategies and technologies for their detection and prevention [12].

c. Overreliance on AI. While AI brings significant benefits, such as process automation and improved risk analysis, overreliance on these technologies can have negative consequences. Specifically, there is a risk of neglecting human judgment and traditional verification methods, which are essential in the context of cybersecurity. Human judgment remains vital for correctly interpreting data and making complex decisions that cannot be

fully managed by AI. Therefore, establishing robust verification processes and educating employees about the potential risks associated with AI use are crucial. These measures ensure that AI does not become a weak point in the security infrastructure but rather a tool complemented by human discernment [13].

To fully harness the potential of AI while maintaining organizational security, continuous vigilance is essential. The implementation of rigorous verification processes and the constant updating of security policies are crucial to protect against the risks associated with AI. Additionally, it is important to promote a culture of awareness among employees, educating them about new types of threats and encouraging them to report suspicious behaviors.

The National Institute of Innovations in Cybersecurity „CYBERCOR" plays a central role in strengthening cybersecurity through a diverse range of activities and innovations essential for protecting digital infrastructure and developing the necessary skills in this critical field. The institution focuses on several strategic areas, including offering specialized courses and certifications designed for public officials, IT professionals, teachers, students, and pupils. These programs are meticulously designed to enhance the cybersecurity skills of participants and to promote the adoption of best practices, such as cyber hygiene, at all levels of society.

In addition to its educational role, the National Institute of Innovations in Cybersecurity „CYBERCOR" is actively engaged in the development and implementation of cybersecurity infrastructures. By collaborating with globally renowned technology partners, the institute gains access to cutting-edge technology, state-of-the-art IT equipment, and top-quality educational resources. These collaborations not only enable the National Institute of Innovations in Cybersecurity „CYBERCOR" to provide specialized training and consulting services but also play a decisive role in forming a body of specialists capable of effectively protecting critical digital information and infrastructures.

Integrating AI into cyber risk management opens up significant opportunities for enhancing security; however, this endeavor requires a well-balanced approach that accurately assesses both the benefits and potential dangers associated with it. The National Institute of Innovations in Cybersecurity „CYBERCOR" understands that only through a careful combination of advanced technology and rigorous human processes can a robust and resilient cybersecurity environment be built.

Through these initiatives, the National Institute of Innovations in Cybersecurity „CYBERCOR" will not only contribute to the development of national capabilities in the field of cybersecurity but will also play a crucial role in strengthening the country's position on the global stage as a leader in innovation and cyber protection. An essential aspect of this strategy is the development of advanced educational content, created in collaboration with renowned technology partners such as Palo Alto, Cisco, and Fortinet.

Collaboration with Palo Alto Networks enables the National Institute of Innovations in Cybersecurity „CYBERCOR" to integrate the latest security technologies into its educational programs, offering courses and hands-on labs that reflect the real-world challenges faced by cybersecurity professionals. Cisco contributes its expertise in networking and IT infrastructures, helping to develop courses that cover both the fundamentals and advanced aspects of network security.

Fortinet, known for its integrated security solutions, adds value by providing educational platforms and resources that allow participants to learn through practical simulations in virtual environments.

These partnerships not only enrich the National Institute of Innovations in Cybersecurity „CYBERCOR" educational offerings but also ensure that graduates are equipped with the necessary skills to meet the challenges of cybersecurity at a global level.

5. The use of AI in security awareness programs

Through these efforts and collaborations, the National Institute of Innovations in Cybersecurity „CYBERCOR" not only trains specialists capable of responding to current challenges in cybersecurity but also contributes to the continuous innovation in methods of training and awareness of cyber threats. In this direction, the use of AI becomes a key element, offering opportunities to personalize and streamline educational programs.

As organizations become increasingly aware of the need to protect their digital resources, the importance of security awareness programs is growing. These programs aim to educate employees about cyber threats and teach them how to recognize and appropriately respond to potential attacks. In this context, AI provides powerful tools to customize and enhance these programs, making them more relevant and impactful for participants.

One of the most valuable uses of AI in security awareness programs is its ability to generate personalized educational content. AI can analyze data related to employee behavior and profiles to create training materials tailored to the specific needs of each department. For example, an employee in the finance department might receive training focused on recognizing phishing attacks specific to their industry, while IT staff might be trained on ways to detect and prevent security breaches.

AI can also be used to create scripts for educational videos, which are among the most effective means of conveying complex information in an easily understandable way. For instance, an AI program could generate a script for a two-minute video explaining what a „vishing" (voice phishing) attack is, how it works, and how employees can protect themselves against it. The script can be simplified to ensure it is understood by employees from all departments, ensuring the message reaches all members of the organization.

In addition to videos, AI can be used to generate quizzes and other training materials that help reinforce the knowledge employees have acquired. For example, an AI system can create a set of multiple-choice questions based on the content of an educational video, providing a quick and efficient way to assess employees' understanding and retention of information. These quizzes can be personalized to focus on previously identified weaknesses in employees' security behavior, ensuring that the training is relevant and effective.

Concrete examples of using AI in security awareness programs

1. **Creating simulated training scenarios.** AI can be used to develop simulated attack scenarios that reflect the current threats facing the organization. These simulations can include phishing attacks, business email compromises, or ransomware attacks, allowing employees to practice appropriate responses in a controlled environment.

2. **Automating feedback.** Another advantage of using AI is the ability to provide instant and personalized feedback to employees after completing quizzes or participating in simulations. AI can analyze responses and suggest additional study materials or training sessions to address identified gaps.

3. **Creating personalized awareness campaigns.** AI can help create security awareness campaigns tailored to different groups within the organization. For example, a campaign for sales staff might focus on protecting customer information, while a campaign for the software development team could emphasize the importance of source code security.

6. Implementation model at National Institute of Innovations in Cybersecurity „CYBERCOR" based on „WHY"

Vision. Training cybersecurity specialists and implementing the most advanced technologies and practices to protect critical resources.

Aligning initiatives with „WHY" through:

a. **Educational programs.** Every course or certification should be designed to develop the necessary skills to effectively protect digital infrastructures. The purpose of each program must be communicated to participants to instill motivation and responsibility for applying knowledge practically and effectively.

b. **Technological projects**. Every technological project, whether it's implementing new security technologies or developing advanced infrastructures, should be justified by its contribution to the National Institute of Innovations in Cybersecurity „CYBERCOR" mission. Technological decisions should be guided by the goal of protecting and strengthening critical networks and systems.

Communication and promotion

a) **Within the Institute**. National Institute of Innovations in Cybersecurity „CYBERCOR" constantly communicates the „WHY" behind each project, program, or initiative to employees and partners. This is achieved through informational sessions, educational materials, and by integrating this concept into the organizational culture.

b) **Externally**. National Institute of Innovations in Cybersecurity „CYBERCOR" promotion on the international stage includes clarifying the institute's purpose and motivation in all presentations and international partnerships. This attracts partners and collaborators who share the same values and goals.

Measuring impact

a) **Performance indicators**. Developing KPIs that measure how well initiatives align with the organization's „WHY". These indicators might include measures of the effectiveness of educational programs, the impact of implemented technologies, and the satisfaction of partners and employees.

b) **Continuous feedback**. Incorporating a feedback system that allows for the constant adjustment and refinement of initiatives to ensure they remain aligned with the National Institute of Innovations in Cybersecurity „CYBERCOR" central purpose.

This model is proposed for implementation at Cybercor as a strategic framework to guide all organizational actions and decisions. Constant alignment with the „WHY" will ensure that each initiative significantly contributes to the organization's mission and vision and that the National Institute of Innovations in Cybersecurity „CYBERCOR" remains at the forefront of innovation in cybersecurity.

By implementing this model, the National Institute of Innovations in Cybersecurity „CYBERCOR" will not only meet its immediate objectives but also build a solid foundation for sustainable development and long-term success in the field of cybersecurity.

Another major advantage of using AI in security awareness programs is the efficiency in content production, especially in organizations with limited resources. AI can automate many tasks related to the creation and distribution of educational content, thus reducing the time and costs needed to keep employees informed and prepared. For example, AI can quickly generate and customize materials for a new security awareness course without requiring extensive intervention from specialist teams.

7. Challenges and limitations of AI in Cybersecurity

Although AI brings numerous advantages in risk management and the creation of security awareness programs, its use is not without significant challenges and limitations. Understanding these limitations is important to maximize the benefits of AI and minimize the associated risks.

One of the main disadvantages of AI is related to the accuracy of its output. AI, particularly machine learning and content generation models, relies on the data it receives and how it is trained. If the initial data is incomplete, biased, or incorrect, the results produced by AI can be inaccurate or even misleading. In the context of cybersecurity, an incorrect analysis or an erroneous automated response can have serious consequences, leading to decisions that could expose the organization to additional risks.

Integrating AI into cybersecurity systems also introduces new security and privacy risks. AI requires access to large volumes of data to function effectively, which may include sensitive or confidential organizational data. If this data is compromised, the organization could suffer significant losses. Additionally, AI itself can become the target of cyber attacks, such as manipulating inputs to cause AI to produce incorrect outputs (adversarial attacks). These attacks can undermine trust in AI systems and lead to additional vulnerabilities within the security infrastructure.

Another sensitive aspect relates to the intellectual property rights over outputs generated by AI. Who owns the rights to a script, image, or video created by an AI model? These questions are still the subject of legal debate and may complicate the use of AI within organizations. Furthermore, there is a risk that AI outputs may violate copyright or be biased if they are based on data sourced from inappropriate or unreliable origins.

To mitigate the risks associated with using AI, organizations must adopt a proactive and well-informed approach:

a. **User education and awareness.** All users must interact with AI - whether they are developers, administrators, or end users - and are aware of its limitations and associated risks. This includes educating employees about potential AI-based attacks and how AI can be used ethically and safely.
b. **Implementing ethical and verification processes.** Organizing solid ethical processes that include the verification of AI outputs and the continuous monitoring of these systems' performance is crucial. These processes should also include measures to ensure compliance with data protection regulations and intellectual property rights.
c. **Testing and validating AI systems.** Before full implementation, AI systems should be rigorously tested to identify any vulnerabilities and to evaluate the accuracy of their outputs. Continuous validation and updating of AI models are necessary to ensure they function correctly and securely.
d. **Adopting a transparency policy.** Organizations should be transparent about their use of AI, explaining how data is used and how automated decisions are made. This transparency will not only help build trust among employees and customers but also facilitate compliance with legal regulations.
e. **Human oversight and intervention.** AI should not be used without human oversight. Critical decisions, especially those involving data security or confidentiality, should include human intervention and validation to prevent possible AI errors.

While AI offers numerous opportunities for enhancing cybersecurity, organizations need to be aware of its challenges and limitations. By implementing proactive measures and

solid ethical processes, organizations can minimize associated risks and fully leverage AI's potential to ensure security and data protection.

8. The impact of AI on security culture

It is essential to explore the impact AI can have on the security culture within organizations. A robust security culture is not just about implementing advanced technologies but also about creating an environment where security is understood, valued, and supported by all employees. AI plays a vital role in facilitating this environment by personalizing training and ensuring continuous workforce engagement in security awareness programs.

One way AI can strengthen security culture is by personalizing learning experiences. Unlike traditional training programs, which often adopt a one-size-fits-all approach, AI enables the creation of customized courses that address the specific needs and behaviors of each employee. For example, an employee working in the finance department might receive training focused on protecting financial data, while an IT employee might benefit from specific training on protecting networks and digital infrastructure.

This personalization not only makes the training more relevant and accessible to employees but also contributes to changing their behavior in ways that support the organization's security objectives. Employees learn to recognize risks specific to their roles and adopt behaviors that mitigate these risks, contributing to the reinforcement of a solid security culture.

AI can also play a crucial role in maintaining continuous employee engagement in security awareness programs. Instead of relying on occasional training sessions, AI can provide constant feedback and real-time updates, helping employees stay informed about the latest threats and best security practices. For example, AI can send personalized notifications when it detects behaviors that might pose a risk or recommend additional training sessions if an employee shows signs of vulnerability to certain types of attacks.

This continuous engagement helps keep security a constant priority within the organization, encouraging a proactive attitude toward protecting resources and data.

AI can be a catalyst for changing workforce behavior in a manner that supports the adoption of a robust security culture. By analyzing past behaviors and anticipating future risks, AI can help organizations implement strategies that encourage safer behavior. For instance, AI can identify behavioral patterns that suggest careless use of sensitive data and suggest specific interventions to correct these behaviors.

Additionally, using cyber attack simulations and other interactive training methods, AI can create learning experiences that are more engaging and effective than traditional methods. At the Technical University of Moldova (UTM), this approach is well integrated into the curricula of IT disciplines, particularly in courses focused on cybersecurity, networks, and digital infrastructures [14-17]. These simulations and interactive methods not only provide students with the opportunity to learn through practice but also allow them to deeply understand the dynamics of cyber attacks and develop essential skills for effectively responding to such threats.

At the National Institute of Innovations in Cybersecurity „CYBERCOR", students and professionals in the field can test authentic situations using real traffic and analyze the behaviors and reactions of systems in real time. National Institute of Innovations in Cybersecurity „CYBERCOR" state-of-the-art infrastructure allows for the simulation of

complex cyberattack scenarios, allowing participants to face challenges similar to those encountered in the real world. This advanced training environment not only enhances participants' technical skills but also develops their ability to make quick and effective decisions in critical situations. Thus, the National Institute of Innovations in Cybersecurity „CYBERCOR" becomes a center of excellence for training cybersecurity specialists, preparing them to meet the challenges they will face in their professional careers.

The goal of integrating these advanced technologies into the curriculum is to train well-prepared specialists who can anticipate and counteract real cyber attacks. Scientific research in emerging technologies such as cybersecurity, privacy, and blockchain has become increasingly important in shaping the future of global innovation, economic competitiveness, and national security [18]. In this way, UTM actively contributes to preparing a new generation of cybersecurity experts ready to protect critical infrastructures both nationally and internationally. This educational approach, based on the practical use of AI and simulations, ensures that students not only acquire theoretical knowledge but also gain relevant practical skills necessary to excel in the continuously evolving field of cybersecurity.

A strong security culture is built not only through policies and technology but also through collective behaviors and attitudes that support security at all levels of the organization. AI, with its ability to personalize and adapt training and awareness programs, plays a crucial role in developing this culture. Employees become not just passive participants in security programs but active partners who understand the importance of security and contribute to protecting the organization against cyber threats. The rapid development of information technologies and the growth of related cyber threats force us to constantly improve the regulatory framework in this area [19-21].

Integrating AI into an organization's security strategy can profoundly impact its security culture. By personalizing training, ensuring continuous engagement, and facilitating behavior change, AI helps create an environment where security is a collective responsibility, thereby protecting the organization from emerging cyber risks.

9. Conclusions

Integrating AI into cyber risk management and awareness programs is not just a technological innovation; it is also a clear manifestation of the importance of starting with „WHY" in any strategic endeavor. In the context of cybersecurity, the „WHY" represents the fundamental motivation that drives organizations to adopt proactive measures and invest in advanced technologies like AI, to protect not only their digital resources but also the integrity and continuity of their operations.

The National Institute of Innovations in Cybersecurity „CYBERCOR", through its initiatives, exemplifies this „WHY" philosophy by focusing not only on the development of security technologies but also on the education and awareness of all participants in the digital security process. A clear understanding of the „WHY" behind their actions protecting critical infrastructure and training professionals capable of meeting future challenges provides direction and meaning to all their efforts.

Thus, combining advanced technology with a well-defined strategy anchored in „WHY" not only enhances the efficiency and resilience of cybersecurity but also ensures that every step taken is aligned with the organization's broader purpose. This clarity of purpose, as highlighted by Sinek, is what will differentiate organizations that not only adopt innovation but do so in a way that has a lasting and significant impact.

This research was conducted with the support of the National Institute of Innovations in Cybersecurity ”CYBERCOR”, part of the Technical University of Moldova. The authors express their gratitude to colleagues and partners for their valuable contributions and collaboration in the development of this study.

Conflicts of interest. The authors declare no conflicts of interest.

References

1. Ponemon Institute. The 2022 Ponemon Report on Cybersecurity Risks. Available online: https://go.proofpoint.com/en-ponemon-report-2022.html (accessed on 13 January 2025).
2. ISO/IEC 27035-1:2023. Information technology – Information Security Incident Management. Available online: https://cdn.standards.iteh.ai/samples/78973/38e0e742e02741ba856510f74aa9f23b/ISO-IEC-27035-1-2023.pdf (accessed on 19 January 2025).
3. Skålén, P.; Gummerus, J.; von Koskull, C.; Magnusson, P.R. Designing value propositions: An exploration and extension of Sinek's 'Golden Circle' model. *Journal of Design Business & Society* 2019, 5(1), pp. 59-76.
4. Willie, M. M. *The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture*. SSRN. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4564291 (accessed on 11 January 2025).
5. NIST incident response plan: Building your own IR process based on NIST guidelines. Incident Response. Available online: https://www.cynet.com/incident-response/nist-incident-response/ (accessed on 7 January 2025).
6. Sinek, S.; Mead, D.; Docker, P. *Find your why: A practical guide for discovering purpose for you and your team*. Portfolio, New York, SUA, 2017, 242 p.
7. Russell, S.; Norvig, P. *Artificial Intelligence: A Modern Approach*. Prentice Hall, NJ, SUA, 2020, 1136 p.
8. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*. MIT Press, Cambridge, MA, USA, 2016, 800 p.
9. Mcafee, A.; Brynjolfsson, E. *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company, NY, USA, 2017, 416 p.
10. Bostrom, N. *Superintelligence: Paths, dangers, strategies*. Oxford University Press, Oxford, UK, 2014, 328 p.
11. Brundage, M. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Available online: https://doi.org/10.48550/arXiv.1802.07228 (accessed on 24 July 2024).
12. Chesney, R.; Citron, D.- K. Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. *Foreign Affairs* 2019, 98(1), pp. 147-155.
13. Smith, B.; Shum, H. The Future Computed: Artificial Intelligence and its Role in Society. Available online: https://news.microsoft.com/uploads/prod/sites/14/2018/02/The-Future-Computed.pdf (accessed on 12 august 2024).
14. Peca, L.; Țurcanu, D. *Computer networks: Practical examples solved to be introduced in computer networks*. Tehnica-UTM, Chisinau, Republic of Moldova, 2022, 188 p.
15. Peca, L.; Țurcanu, D. Network security: Practical examples solved to be introduced in network security. Tehnica-UTM, Chisinau, Republic of Moldova, 2023, 243 p.
16. Dumbraveanu, R.; Peca, L. E-learning in Developing ICT Skills of Future Engineers. In: *1st International Online Scientific Conference ICT in Life*, Osijek, Croația, 2022, pp. 86-95.
17. Peca, L. The power of eLearning from promises to practices applied in engineering. *Journal of Social Sciences* 2023, 6(1), pp. 69-80.
18. Bran, E.; Rughinis, R.; Turcanu, D.; Stăiculescu, A. R. Decoding National Innovation Capacities: A Comparative Analysis of Publication Patterns in Cybersecurity, Privacy, and Blockchain. *Applied Sciences* 2024, 14, 7086.
19. Turcanu, D.; Spinu, N.; Popovici, S.; Turcanu, T. Cybersecurity of the Republic of Moldova: A Retrospective for the Period 2015-2020. *Journal of Social Sciences* 2021, 4(1), pp. 74-83.
20. Action list for developing a computer security incident response team (CSIRT). Available online: https://insights.sei.cmu.edu/library/action-list-for-developing-a-computer-security-incident-response-team-csirt/ (accessed on 13 January 2025).
21. Thailand Cybersecurity Act 2019 (English Translation). Available online: https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf. (accessed on 13 January 2025).

Citation: Peca, L.; Ţurcanu, D. Reducing cyber risk through a human–centred approach. *Journal of Engineering Science*. 2025, XXXII (1), pp. 18-31. https://doi.org/10.52326/jss.utm.2025.8(2).02.

Publisher's Note: JES stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright:© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Submission of manuscripts: jes@meridian.utm.md