Online-Journals.org

iJEP International Journal of Engineering Pedagogy

iJEP | eISSN: 2192-4880 | Vol. 16 No. 5 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijep.v16i5.60763

PAPER

Strategic Importance of Education in Cybersecurity

Pavel Beňo[1] (✉), **Roman Hrmo**[2]

[1]Comenius University in Bratislava, Bratislava, Slovakia

[2]DTI University, Dubnica nad Váhom, Slovakia

pavel.beno@uniba.sk

ABSTRACT

This paper examines the strategic importance of cybersecurity education as a pedagogical and managerial mechanism for strengthening organisational resilience. Responding to the need for practice-orientated engineering pedagogy, the paper formulates a guiding research question: How can role-specific cybersecurity education be selected, justified, and evaluated so that it supports resilient behaviour across organisational levels? The study combines a structured narrative review of cybersecurity education and awareness approaches with a transparent SWOT-based analytical framework. SWOT is used as a managerial self-assessment tool for identifying strengths, weaknesses, opportunities, and threats in both the general cybersecurity environment and the human-factor dimension. The paper distinguishes gamification from games, explains the rationale for selecting educational approaches, and proposes operational criteria for translating SWOT findings into training requirements. The contribution is intended for educators, cybersecurity managers, and organisational leaders who design or evaluate cybersecurity awareness programmes in engineering-orientated, technical, and socio-technical environments.

KEYWORDS

cyber security, cybersecurity education, engineering pedagogy, SWOT, security awareness

1 INTRODUCTION – CYBERSECURITY AS A STRATEGIC PRIORITY

We constantly speak of the growing trend of cybercrime, and new reports of attacks on various sectors appear in the media on a regular basis. The most recent large-scale example is the company Jaguar, which has been unable to restore its production lines distributed across the globe for more than three weeks. In today's digitally interconnected world, the dependence of organisations on information technologies is growing almost exponentially. Along with this dependence, cyber threats are also intensifying.

Nextech [1] reports a twofold increase in attacks in the first half of 2025. These include sophisticated phishing attacks and ransomware, as well as threats stemming from employee errors. In today's world—the world of AI—such attacks are becoming increasingly sophisticated, with hackers making ever greater use of AI-based tools.

Beňo, P., Hrmo, R. (2026). Strategic Importance of Education in Cybersecurity. *International Journal of Engineering Pedagogy (iJEP)*, 16(5), pp. 28–45. https://doi.org/10.3991/ijep.v16i5.60763

Article submitted 2026-01-26. Revision uploaded 2026-05-31. Final acceptance 2026-06-21.

© 2026 by the authors of this article. Published under CC-BY.

Security incidents are no longer merely an issue for the IT sector; their consequences can disrupt the daily operations of a company, jeopardise its reputation, undermine financial stability, and erode customer trust [2].

Companies adopt various forms of protection. Most commonly, they safeguard themselves by implementing modern firewalls, so-called next-generation firewalls, and by deploying new antivirus solutions. Organisations also increasingly rely on the encryption of sensitive data; backup through non-rewritable storage known by the acronym WORM (Write Once – Read Many); introduce multi-level authentication; and regularly test the resilience of their systems through penetration testing and diverse simulations of cyberattacks.

Another crucial element of cybersecurity is the education of employees and management. This must be carried out systematically, starting from basic awareness of risks, through training in phishing recognition, to the strategic management of incidents. ESET, as one of the globally recognised leaders in the field of cybersecurity, posed the following questions regarding the necessity of cybersecurity training [3]:

- You educate employees and foster security awareness within the organisation.
- You protect your company against the threats and pitfalls of cyberspace.
- You increase your company's ability to withstand cyber threats.
- You minimise the chances of attackers succeeding in their attempts.

According to the IBM *Cost of a Data Breach Report 2025* [4], a data breach in 2025 costs organisations an average of 4.44 million USD, while in the United States alone the figure has risen to as much as 10.22 million USD. The report also highlights the growing risks associated with artificial intelligence (AI) and so-called *shadow AI*, referring to unauthorised implementations of AI within organisations. Similarly, the National Security Authority of the Slovak Republic (NBU SR) [5] has issued warnings regarding threats linked to the use of certain AI models.

Already two years ago, the same IBM report [6] stated that the most common causes of data breaches were employee errors or misconfigured systems. Summarising the findings, it becomes evident that as many as 82% of incidents involve elements of the human factor. This indicates that technological solutions alone are insufficient when confronted with mistakes or a lack of employee awareness. Building a security culture and investing in education have therefore become indispensable.

For the reasons mentioned above, the role of the cyber security manager (CSM) in building security awareness is strategically irreplaceable. The CSM sets security standards and cyber security policies but, above all, fosters a culture in which cybersecurity becomes an integral part of the daily work of all employees. According to the ISACA *People, Processes and Behaviours 2022* report [7], it is crucial for companies that leadership actively supports a security culture and employee education, since the human factor remains one of the main causes of security incidents.

The objective of this article is to strengthen the pedagogical framing of cybersecurity education in organisations and to provide a transparent approach for linking educational interventions to organisational resilience. The paper addresses the following research question: RQ1: Which role-specific cybersecurity education approaches can be selected and justified through SWOT-based organisational self-assessment in order to improve resilience and security culture? Two supporting questions guide the analysis: RQ1a: What educational approaches are suitable for management, administrative staff, and technical employees? RQ1b: Which criteria should managers use when translating SWOT findings into actionable training requirements? The target audience consists of engineering educators, cybersecurity managers, adult-learning designers, and decision-makers responsible for building

security awareness in organisations. The contribution is not an experimental evaluation of one training programme; rather, it is a practice-orientated pedagogical framework that connects related work, organisational analysis, and implementation guidelines.

2 RELATED WORK AND PEDAGOGICAL POSITIONING

Cybersecurity education has increasingly been studied as a socio-technical and pedagogical challenge rather than only as a matter of technical control. Systematic reviews show that organisations use a wide range of approaches, including awareness campaigns, e-learning, microlearning, simulations, phishing exercises, cyber ranges, serious games, and blended learning. However, the effectiveness of these approaches depends on context, learner characteristics, timing, feedback, and the extent to which training is connected with real work tasks [8] [9] [10].

For this reason, the paper positions cybersecurity education within engineering pedagogy as a form of competence-orientated learning. In technical and engineering environments, employees must not only know rules but also understand systems, risks, dependencies, and consequences. This corresponds with the NIST NICE Framework, which describes cybersecurity work through tasks, knowledge, skills, and abilities and can therefore support role-specific training requirements [11].

The literature also cautions against treating security awareness training as automatically effective. Phishing simulations, for example, may improve recognition and reporting when they are embedded in a broader learning process with timely feedback, but isolated or punitive simulations can produce limited learning effects, stress, or even mistrust. Therefore, such simulations should be used as diagnostic and reflective tools rather than as stand-alone proof of competence [9] [12].

Finally, it is important to distinguish gamification from games. Gamification refers to the use of game design elements, such as points, feedback, badges, progression, or challenges, in a non-game context; serious games are complete game-based learning environments. Both may support motivation and engagement, but they require explicit learning objectives and evaluation criteria [13] [14]. This distinction is used in the present paper when discussing interactive cybersecurity education.

3 WHY MANAGERS MUST CARE ABOUT EDUCATION IN THE FIELD OF CYBER SECURITY

As outlined in the introduction, this work sets the direction of our research and its focus area. The times when cybersecurity was perceived merely as an issue of the IT department are long gone. Over the past decade, cybersecurity has increasingly become a strategic component of the management of every organisation. For managers, this means that education in the field of cybersecurity is essential not only for employees but also for senior management.

It can be stated that although managers may delegate a significant portion of responsibilities to the CSM, they still bear their own accountability for the organisation. This accountability translates into several reasons why managers must be aware of the state and level of cybersecurity within their organisation:

- Responsibility for risk management
- Reputation, business continuity and legislation
- Financial consequences of incidents and the importance of the human factor

3.1 Responsibility for risk management

The ultimate responsibility for risk management—encompassing not only financial and operational aspects within the company—rests with the managers themselves. Cyber incidents can affect the entire business, causing operational disruptions, data loss, or the misuse of sensitive information. The ability to identify vulnerabilities, understand the types of threats, and implement appropriate measures enables managers to make decisions that minimise the impact of such incidents. Risk management in the context of cybersecurity involves several key areas:

- Identification and threat assessment – A manager must be able to identify potential sources of risk, whether external (malware, phishing, etc.) or internal (user errors, unauthorised access to data, etc.). Equally important is the ability to understand the likelihood of an incident and its potential impact on the company's operations, finances, and overall reputation.
- Prioritisation and Resource Allocation – A manager must determine which risks are critical and require immediate attention, which can be addressed later, and which may be acceptable to leave unresolved. This is referred to as the level of residual risk. To this end, the manager must also ensure the adequate allocation of resources—whether in the form of investments in technologies, external audits, the engagement of specialised consultants, or employee training.
- Implementation of Security Measures and Policies – This involves direct actions aimed at eliminating risks. The manager establishes guidelines that define how sensitive data is handled, how systems are monitored, and how incidents are to be addressed in the event they occur.
- Monitoring and Continuous Improvement – It is essential to ensure that the implemented measures are regularly reviewed in terms of their effectiveness, that new and constantly evolving threats are assessed, and that company strategies are adapted accordingly. This represents an ongoing process of improvement.
- Accountability in the Event of Incidents – It must be recognised that in the case of incidents, the manager bears both legal and moral responsibility for the decisions that influence their impact on the company.

The Ability to Respond Quickly and Effectively – A manager's capacity to activate a crisis plan and communicate with all stakeholders can significantly minimise damages and help maintain the trust of customers and partners.

3.2 Reputation, business continuity and legislation

A security incident can significantly damage the trust of a company's customers and partners. Corporate clients, business partners, and investors expect that their data—particularly sensitive information—is adequately protected and that the company is capable of managing risks. In the commercial world, a company's reputation carries direct financial value, and a data breach or major service outage can lead to a loss of customer trust, which may translate into reduced revenues. According to PwC's Annual Global Digital Trust Insights Survey [15], among the damages organisations have suffered over the past three years as a result of cyberattacks or data breaches are customer loss (27%), loss of client data (25%), and damage to reputation or brand (23%).

Since cyberattacks can paralyse critical systems and disrupt the entire operation of a company, managers must be able to ensure business continuity (BC). BC is achieved through the implementation of disaster recovery plans (DRP) and the regular testing of backup systems and procedures, as well as by increasing the resilience of processes against cyber threats.

Moreover, legislative frameworks such as GDPR [16] or the more recent NIS2 Directive [17] impose obligations on companies in the areas of data protection and incident prevention. Compliance with legislation is not only a legal requirement but also a mechanism that fosters trust among customers and business partners. Conversely, non-compliance with these regulations can result in significant fines and legal consequences, thereby increasing the pressure on management to actively support security education. A manager who understands the regulatory framework is able to ensure the alignment of internal processes with legal requirements, minimise the risk of substantial penalties, and proactively plan investments in security technologies and training.

3.3 Financial consequences of incidents and the meaning of the human factor

Cyberattacks, as well as internal errors, often have both immediate and long-term financial impacts. These include not only the direct costs of remediation but also indirect damages that may arise over time. Among them are expenses related to system recovery, legal services, fines, and the long-term consequences of customer loss. We can therefore state that this represents a form of:

- Direct Costs – These are associated with the restoration of IT systems, servers, and data, as well as legal services and court fees, payments for security audits, or the services of external specialists.
- Indirect Costs – These include the loss of customers or business partners and revenue declines caused by operational disruptions, as well as damage to brand and reputation, which may negatively affect future business opportunities.
- Long-Term Consequences – Reported incidents may result in fines related to legislation, for example, in cases of personal data theft; increased premiums for cyber risk insurance; as well as long-term internal investments directed toward technologies and training aimed at minimising future risks.

A significant share of cybersecurity incidents stems from human errors linked to insufficient awareness, commonly referred to as the human factor. This clearly demonstrates that technological solutions alone are insufficient; rather, education and a strong security culture within the company are considered essential.

An educated manager is capable not only of responding to incidents but, above all, of preventing them, implementing effective policies, and fostering a culture in which security is not merely a rule but a natural part of every employee's work.

4 METHODOLOGY AND ANALYTICAL PROCEDURE

The paper uses a conceptual and practice-orientated methodology. First, it summarises relevant literature on cybersecurity education, adult learning, gamification, simulations, and organisational security culture. Second, it derives role-specific

educational requirements for three learner groups: management, administrative staff, and technical employees. Third, it applies SWOT analysis as a structured self-assessment tool for identifying educational and organisational priorities. Fourth, it translates the SWOT findings into operational recommendations that can be used when selecting training formats.

The SWOT analysis is not presented as a statistical measurement. Its purpose is to support reproducible managerial reasoning by making explicit which factors are considered internal strengths and weaknesses and which factors are interpreted as external opportunities and threats. In practice, each item should be scored by an organisation according to likelihood, impact, and current control maturity. The resulting priorities should then be validated through security audits, incident records, phishing-reporting statistics, employee surveys, and interviews with process owners.

To improve transparency, the following criteria guided the selection of educational approaches: role relevance, transfer to daily work, measurability of learning outcomes, feasibility for the organisation, alignment with legal and governance requirements, and contribution to resilience. These criteria provide a rationale for the recommendations and reduce the risk that the proposed measures appear arbitrary.

Table 1. Criteria for selecting and evaluating cybersecurity education approaches

Criterion	Meaning for Selecting Cybersecurity Education	Example of Operational Indicator
Role relevance	The approach fits the tasks and risk exposure of the learner group.	Separate learning paths for management, administrative staff, and technical staff.
Transfer to daily work	Training must support behaviour employees can apply immediately.	Ability to report suspicious emails, use MFA correctly, or follow incident procedures.
Measurability	The outcome can be evaluated without relying only on attendance.	Pre/post tests, reporting rates, exercise performance, observed compliance.
Feasibility	The approach is realistic in terms of time, cost, and available expertise.	Short modules for all staff; deeper simulations for high-risk roles.
Governance alignment	Training supports policies, legislation, and managerial accountability.	Coverage of GDPR, NIS2, incident reporting, and internal procedures.
Resilience contribution	The approach strengthens prevention, detection, response, or recovery.	Lower repeated errors; faster escalation; improved crisis coordination.

5 SWOT ANALYSIS OF CYBERSECURITY FROM THE PERSPECTIVE OF THE ORGANISATION

As we have noted, cybersecurity is currently one of the key areas influencing not only the technological resilience of a company but also its reputational and legal accountability. The size of the organisation is by no means a decisive factor. Statistically, attacks are more often directed at small and medium-sized enterprises, which generally lack well-developed protective mechanisms. Attackers attempt to exploit a wide range of technical and configuration vulnerabilities, as well as human ignorance, in order to infiltrate systems, gain access to devices and sensitive data, and ultimately disrupt the company's operations.

A good manager sets as a goal the regular evaluation of the state of cybersecurity and the following:

- Determine the actual state of security within the company
- Identify the greatest risks and vulnerabilities
- Propose specific measures to minimise risks
- Strive to raise awareness among employees and management about the importance of security measures within the organisation

In this work, we employ the well-known SWOT analysis, a tool familiar to managers, which makes it possible to evaluate the state of cybersecurity comprehensively and clearly through four categories:

- S – Strengths: It addresses what we do well and which security mechanisms are functioning effectively.
- W – Weaknesses: It identifies where deficiencies or vulnerabilities exist.
- O – Opportunities: It defines the opportunities for improvement or innovation.
- T – Threats: It is a list of factors that may threaten us, whether from external or internal sources.

In this work, we present two SWOT analyses that we developed and applied in assessing the state of cybersecurity within organisations. Due to the limited scope of this contribution, we will not provide a specific analysis of a selected company but will instead describe a practical approach to the activities required to achieve a thorough analysis. The first is a SWOT analysis of the general level of cybersecurity within a company, while the second is a SWOT analysis focused on the human factor, that is, the determination of awareness and knowledge of cybersecurity within the organisation. It is the latter analysis that interests us most, as this work is orientated toward the strategic significance of education. Naturally, it is possible to create a dedicated SWOT methodology for each distinct area of cybersecurity.

The context assumed for the SWOT examples is a small- or medium-sized organisation that depends on digital services, processes personal or business-critical data, and must comply with internal governance and external cybersecurity requirements. The listed factors should therefore be interpreted as a reusable analytical template rather than as findings from one named organisation. To apply the template reproducibly, organisations should document the evidence for each item, assign a priority score, identify the responsible owner, and define a related educational or technical response.

5.1 SWOT analyses – General level of the state of cyber security

S – strengths

- Use of modern IT infrastructure and regular renewal
- Existence of an internal team with certifications (ISO27001, CISSP, etc.)
- Implemented security policies
- Centralisation at the level of identity and access management (SSO, MFA, etc.)
- Cooperation with external companies for audits and consultations
- Regular penetration testing and the presence of SIEM monitoring

W – weaknesses

- Lack of professional staff for cybersecurity and overall IT
- Absence of an Incident Response Plan (IRP)
- Outdated, unpatched applications and unsupported hardware
- Underestimation of risks related to cloud services
- Low level of cybersecurity awareness, especially outside the IT department
- Non-compliance with applicable legislation (GDPR, Cybersecurity Act, and NIS2)

O – opportunities

- Availability of grants or state support for cybersecurity
- Integration of cybersecurity training as part of corporate culture
- Cooperation with CSIRTs or other MSSPs (Managed Security Service Providers)
- Automation of security processes, such as patch management
- Reduction of reputational risk through preventive measures

T – threats

- Ransomware, phishing, BEC (business email compromise)
- Leakage of sensitive or personal data
- Increase in fraud facilitated by AI (deepfake, voice spoofing, etc.)
- Deliberate as well as unintentional insider threats
- Stricter regulations arising from legislative changes
- Suppliers as a weak link in the chain

5.2 SWOT analyses – human factor

S – strengths

- High willingness of employees to participate in organised training
- Opportunity to utilise both internal and external training programmes
- Employees are aware and understand the value of corporate data.
- Security campaigns aimed at raising risk awareness

W – weaknesses

- Responses to fraudulent emails (phishing)
- Reusing the same passwords across multiple platforms
- Delaying device updates
- Failure to comply with internal policies
- Exposure to social engineering
- Low involvement of departments outside IT (finance, HR, etc.)

O – opportunities

- Implementation of simulated phishing campaigns
- Interactive training (gamified, e-learning, etc.)
- Internal cyber security ambassadors

- Integration with the company's social responsibility initiatives
- Feedback from real incident, so-called case studies

T – threats

- Employees as the "weakest link" (human factor)
- Attacks targeting specific individuals (spear phishing, whaling)
- Unintentional data leaks, use of public Wi-Fi
- Unsecured home office setups
- Employee overload leading to mistakes and inattentiveness
- Employees facing personal difficulties being more prone to errors

Table 2. Example of translating SWOT findings into education requirements

SWOT Finding	Evidence to Document	Training Requirement	Evaluation Measure
Low awareness outside IT	Survey results, helpdesk tickets, audit findings	Role-specific microlearning and workshops for non-IT departments	Knowledge test and incident-reporting rate
Responses to phishing emails	Simulation results and real reports	Reflective phishing exercises with immediate feedback	Click rate, report rate, repeated-error rate
Management crisis decisions	Incident drill observations	Table-top exercises for leadership and communication	Time to decision and quality of escalation
Unsecured home office	Remote-access audit, BYOD inventory	Short modules on MFA, secure Wi-Fi, and device updates	Compliance checks and policy acceptance
AI-enabled fraud	Threat intelligence and incident examples	Scenario-based learning on deepfakes and voice spoofing	Scenario recognition and escalation accuracy

The advantage of using SWOT analysis is that it:

- Enables the integration of technical and non-technical aspects of security
- Provides a clear presentation of results for both management and company leadership
- Supports strategic planning of security measures and investments
- Can be easily adapted to various segments, from infrastructure to employee training.

Thus, the use of SWOT analysis in assessing the state of cyber security (including self-assessment pursuant to §29, paragraph 1 of Act No. 69/2018 Coll. on Cyber Security and on Amendments to Certain Acts of the Slovak Republic) can provide companies with a clear and effective tool for identifying key areas requiring management's attention. At the same time, it can serve as a starting point for the implementation of concrete measures and for raising cybersecurity awareness across the entire organisation.

6 HOW TO EFFECTIVELY EDUCATE EMPLOYEES

One of the key pillars of building a resilient and adaptable organisation is effective employee education. We believe that all global experts on cybersecurity would agree with this statement. Simply conveying new information is far from sufficient; rather,

it is essential to ensure its transfer into everyday practice, resulting in the long-term development of internal teams. Naturally, the educational needs of employees differ depending on their job position and level of responsibility. These can be categorised by level and role:

- Technical staff, who require more practical training and detailed procedures in order to respond more quickly to specific situations and to effectively use targeted tools.
- Administrative staff, who need to acquire skills in processes, communication, and the use of documentation while also focusing on the ability to coordinate and support other teams.
- Management, which must be orientated toward strategic leadership, decision-making in crisis situations, and the ability to create an environment in which knowledge is effectively disseminated among all employees.

Effective corporate education must be grounded in the principles of andragogy (adult learning) [18] [19], which emphasise practicality, immediate applicability, and the connection to the professional experience of course participants. Modern methods therefore aim to create interactive and experiential forms of learning that replace outdated, unengaging approaches based on passive information intake.

- Microlearning encompasses learning activities that are carried out on a small scale or within a limited time frame [20]. Information is delivered in short, thematically coherent modules, typically lasting 2 to 5 minutes, which increases retention rates and enables more flexible learning. For cybersecurity, this format is more effective in quickly adopting factors, procedures, and updates that might otherwise be lost within the vast volume of information in traditional, more extensive training [21]. *Practical application*: Short videos or learning modules can be used for the rapid adoption of new security rules, familiarisation with software updates, or changes in internal regulations.

The educational value of microlearning is highest when short modules are connected to concrete behaviours and repeated over time. Therefore, microlearning should not replace deeper training for high-risk roles but should serve as a reinforcement mechanism for rules, updates, and recurring mistakes identified through audits or incident reports.

- Simulation exercises are based on the concept of experiential learning, where participants acquire knowledge through experience, reflection, and application of insights in a controlled environment. A typical example requiring adaptation of the real work environment includes tasks whose mastery—or even learning their basics under operational conditions—disproportionately increases risk [22]. In the case of cybersecurity, the risk of potential system compromise is substantial, which makes it appropriate to train users and managers in a simulated environment where such risks do not exist. *Practical application*: In the field of cybersecurity, two teams can be created (the so-called red team vs blue team) to test each other's preparedness and response capability during an attack. Similarly, model exercises can be designed to practise correct procedures in the event of a data breach, for crisis management leadership, and, most importantly, for the simulation of strategic decision-making.

In this paper, phishing simulations and table-top incident exercises are treated as pedagogical interventions only when they include preparation, feedback, reflection, and follow-up learning. Their purpose is not to shame employees but to identify risky situations, support reporting behaviour, and provide evidence for targeted training improvements [23] [26].

- Internal workshops enable colleagues to share experiences and foster a so-called community of practice. This concept, introduced by Wenger [23], describes a setting where knowledge spreads organically and new procedures are developed, tailored to the specific context of the organisation. Workshops also serve as a highly effective managerial tool for supporting corporate culture and strengthening team identity. *Practical application*: They are ideal for sharing experiences across departments. For example, the IT department may present new security procedures, or company leadership may introduce new strategies and discuss their implementation with teams.
- Blended learning combines physical and digital learning in a conscious and integrated way. The aim of blended learning is to shape education in such a way that it becomes more effective, efficient and flexible with the help of IT [24]. In cybersecurity education, this approach is grounded in the theory of blended learning, which combines the advantages of self-directed study—such as learning pace and flexibility—with those of collective learning, where feedback and discussion with the instructor provide significant opportunities for knowledge transfer. *Practical application*: A typical example may be the combination of an e-learning module (e.g., a Moodle course) on GDPR, NIS2, or the Cyber Security Act, together with a workshop where employees practise solving specific case studies.
- Gamification of education refers to the use of game elements in a non-game context [25]. In teaching, gamification is applied as a stimulating tool for learners, aiming to make the learning process more engaging, interactive, and enjoyable. By incorporating gamification, it is possible to increase interest in cybersecurity training and make the learning experience more entertaining [26]. For managers, it is important to carefully plan the introduction of such games. This plan must be based on clearly defined goals, since all objectives and tools work effectively only if participants experience genuine engagement and motivation from the game [27]. In the context of cybersecurity education, this represents one of the manager's most important tasks. *Practical application*: An example we use is the implementation of company challenges, where employees collect points for completing security quizzes. This serves as a motivational tool for fostering a culture of continuous learning.

For clarity, gamification does not mean that the whole training becomes a game. It means that selected game design elements are added to a non-game learning process. Serious games or cyber-range games are separate formats that require more extensive design, scenarios, and evaluation. Managers should therefore select gamification when the aim is motivation and reinforcement, and serious games or simulations when the aim is deeper experiential learning.

- Mentoring and coaching as personalised approaches provided by more experienced colleagues or an external coach are based on Bandura's principles of social learning [28] [29], where observation, modelling, and feedback form the

foundation. Coaching fosters self-reflection and critical thinking, while mentoring also transfers cultural and informal organisational knowledge, which then reflects the overall perception of cybersecurity within the company. *Practical application*: New employees are assigned a mentor who guides them and imparts not only knowledge but also corporate values. Coaching is used primarily in leadership, aimed at developing leadership competencies, the ability to make quick decisions under pressure, and crisis management skills.

By combining these forms appropriately, it is possible to achieve greater retention and transfer of knowledge into practice than would be the case with traditional training. The manager must evaluate the benefits of education and establish measurable indicators. In this way, they can implement the following:

Table 3. Linking learner groups, education approaches and measurable outcomes

Learner Group	Main Learning Need	Suitable Approach	Measurable Outcome
Top management	Strategic risk ownership, legal duties, crisis decisions	Table-top exercises, executive briefings, incident simulations	Decision quality, escalation time, approval of resources
Middle management	Policy implementation and team behaviour	Workshops, case studies, peer discussion	Team compliance, reporting culture, completed action plans
Administrative staff	Recognition of phishing, data handling, reporting	Microlearning, blended learning, reflective phishing simulations	Reporting rate, lower repeated mistakes, test results
Technical staff	Incident response, configuration, secure operations	Hands-on labs, cyber ranges, mentoring	Exercise performance, recovery time, reduced misconfiguration
New employees	Onboarding into security culture	Mentoring, short modules, role-specific checklists	Completion of onboarding and correct use of procedures

- Regular knowledge testing
- Monitoring success in solving model situations
- Gathering feedback from participants as well as their supervisors
- Evaluating team collaboration during stress-related tasks

Naturally, the manager must evaluate not only individuals but also sub-teams and the team as a whole. A suitable approach in this regard is the use of exercises that test employees' ability to function under pressure, collaborate effectively, and maintain process continuity even during unexpected events.

Today, the possibilities for employee education are highly diverse—ranging from internal workshops, e-learning platforms, and mentoring to cooperation with external experts or universities. The foundation for securing qualified employees is laid primarily within the educational process at universities, which shape young people (potential employees) and provide high-quality education in the field of security [30]. For a manager, it is essential to establish a systematic framework in which educational methods are appropriately combined and adapted to the needs of different employee groups and, subsequently, to the company as a whole. Only in this way does education become not merely an obligation but a natural part of corporate culture and a key factor in the organisation's long-term competitiveness.

7 SECURITY CULTURE AS A PART OF STRATEGY OF A COMPANY

Effective employee education forms the foundation for building resilient teams and, consequently, a resilient organisation as a whole. However, the process does not end with the one-time acquisition of knowledge; it is equally important to verify it, conduct regular testing, and create conditions in which employees can retain new insights and apply them in practice. For this reason, the next step is to focus on methods of measuring learning outcomes and evaluating the readiness of teams to face real-world challenges.

Security culture is increasingly becoming an inseparable part of corporate strategy. It can be understood as a set of fundamental assumptions, values, norms, rules, symbols, and beliefs that shape the perception of challenges, opportunities, and risks, as well as the ways in which security is understood and considered. This also encompasses the related methods and patterns of learned behaviour and interaction among social actors, aimed at ensuring the safe continuity and development of all reference entities and of society as a whole [31].

In the field of security, it is no longer just about technical measures or rules in internal guidelines, nor is it solely a matter for IT departments. All measures and their effectiveness depend—and will continue to depend—primarily on people's attitudes, their motivation, their stance, and their everyday behaviour. The task of the organisation is therefore to create an environment in which security becomes a natural value and an integral part of corporate identity. The manager plays a key role in building security culture, demonstrating through their own behaviour the importance of compliance with rules and the proper approach to risks. If a leader disregards internal procedures, they cannot expect employees to respect them. Conversely, if a manager actively communicates about security topics, supports employees in reporting incidents, and rewards safe behaviour, they foster an atmosphere of trust. In such a setting, security becomes a shared responsibility rather than an imposed obligation.

Security culture in a company does not emerge solely through top-down management. It requires acceptance, commitment and support (buy-in) across the entire organisation. In short, employees at all levels must understand why security matters, what it means for their daily work and what it implies for them personally. For this reason, communication must be clear, understandable, and focused on benefits, not just sanctions. Likewise, it is important to employ modern methods such as gamification, interactive training, and simulations, which actively engage people in security issues. This also helps ensure that security measures are not perceived as an administrative burden but rather as a natural part of business processes.

The security culture of a company is closely connected to the concept of ESG—environment, social and governance. The core idea of ESG may bring tangible benefits in the financing of sustainable activities, which is also reflected in EU legislation. This gradually creates pressure for ESG reporting even among entities not directly bound by such legal obligations [32]. Within the "governance" dimension, emphasis is placed on transparency, risk management, and ethical conduct. In the Slovak Republic, this is embedded in Act No. 69/2018 on Cyber Security [33], as amended by Act No. 366/2024 Coll. [34], effective from January 1, 2025, along with NBU Decree No. 226/2025 Coll. [35] on reporting requirements and NBU Decree No. 227/2025 Coll. [36] on security measures. All of these laws and decrees reflect Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and

repealing Directive (EU) 2016/1148 (NIS2 Directive) [37]. Organisations that work systematically on building security awareness thereby, strengthen not only their internal stability but also their credibility with customers, partners and investors, while also ensuring compliance with legal requirements.

Responsibility in the field of cybersecurity also carries a broader social dimension in preventing incidents that could negatively affect communities or harm the public interest. In this sense, security culture becomes not only an internal tool but also part of the organisation's social responsibility. Security culture is a long-term process that requires leadership commitment, the involvement of all employees, and strategic anchoring within corporate policy. An organisation that understands security as a value rather than merely an obligation gains not only higher resilience against risks but also a competitive advantage in the eyes of the market and society at large.

8 DISCUSSION AND THREATS TO VALIDITY

The analysis suggests that cybersecurity education should be understood as a continuous pedagogical process linked to organisational risk management. The central result is not a universal list of training formats but a set of criteria for selecting and evaluating formats according to learner roles, organisational weaknesses, and resilience objectives. This addresses the practical problem that many organisations conduct security training as a formal compliance activity without demonstrating how it changes behaviour or supports incident readiness.

The SWOT framework is useful because it creates a common language for managers, technical staff, and educators. Nevertheless, SWOT has limitations. It can oversimplify complex socio-technical problems and may reflect the perceptions of the people involved in the assessment. Therefore, a SWOT analysis should be treated as a starting point and combined with empirical evidence such as audit logs, incident data, exercise results, and employee feedback.

The validity of the proposed framework is limited by the fact that it is conceptual and has not been tested in one controlled organisational case. The paper therefore does not claim causal evidence that a particular training method will reduce incidents in every context. Future work should apply the framework in a specific organisation, collect pre- and post-training data, and compare the effectiveness of different educational interventions across roles.

9 WHAT IS POSSIBLE TO DO IMMEDIATELY?

Building a security culture within a company is a long-term process, yet there are steps that managers can implement immediately. These activities not only strengthen the level of cybersecurity within the organisation but also send a clear signal that education and awareness are of strategic importance for stability and competitiveness.

First and foremost, it is necessary to create a systematic training plan that should cover not only technical staff, administrative employees, and management but also the CSM himself or herself. Leaders who actively educate themselves in cybersecurity set an example for others and demonstrate that it is a priority for the entire organisation. After all, an organisation's security is only as strong as its weakest link. Although this comparison may not be pleasant, it unfortunately reflects reality.

A weakness in the form of a user disclosing their login credentials in a phishing campaign can bring down any company, just as a misconfiguration caused by a technical oversight can. Therefore, it is essential to identify weaknesses in time, whether in technical knowledge, appropriate responses to phishing campaigns, or understanding of internal procedures. Identifying such weaknesses enables education to be targeted where it delivers the greatest benefit.

For better managerial orientation, it is advisable to begin with a security awareness audit. Such an audit provides an objective picture of how well employees understand risks and whether they are able to respond adequately. In addition to a traditional security audit, which can be carried out through self-assessment or by an external entity, managers can conduct phishing simulations, short questionnaires, or incident drills. What matters most is the outcome of these evaluations, which must serve as a basis for targeted training and the improvement of processes.

Another key point is the support of the security specialist—ideally, the cybersecurity manager. It is important that the manager not only formally approves but also actively supports their work. This involves ensuring that the CSM has space to communicate with the team, that leadership legitimises their recommendations and that sufficient resources are allocated for the implementation of measures. Such support reinforces the perception of security as a strategic priority and helps reduce the risk of measures remaining only on paper.

Even small and immediate measures can have a profound impact on the future preparedness of an organisation. Training, audits, and systematic support of specialists create the foundation on which long-term development can be built. Companies that implement security activities without delay gain a significant advantage: not only do they achieve better protection against incidents, but they also build stronger credibility with clients, partners and regulatory authorities.

The answer to the question of what an organisation can do immediately is the following:

- Develop a role-specific training plan based on risk exposure, legal duties and prior incident evidence.
- Identify and score the most significant weaknesses using evidence from audits, simulations, surveys and incident records.
- Initiate a security awareness audit with measurable indicators such as reporting rate, click rate, knowledge test results and escalation time.
- Support the security specialist by giving the cybersecurity manager authority, resources and access to management decision-making.

10 CONCLUSION

Effective cybersecurity education is not a one-time activity but a long-term pedagogical process that must reflect the responsibilities, prior knowledge and risk exposure of different learner groups. The paper contributes a practice-orientated framework that links related work, SWOT-based self-assessment, learner roles, educational approaches and measurable outcomes.

The most successful organisations are those that manage to connect theory with practice and create an environment in which education becomes a natural part of corporate culture. It is crucial, especially for leadership, to understand that education is not an expense but an investment—an investment in the stability, reputation and credibility of the organisation. Every euro invested in employee development pays

off in the form of lower incident risk, greater efficiency and better readiness to face increasingly complex challenges. Cyber security thus begins with corporate management. Leaders set the tone, shape the culture and, by their example, determine whether security measures will truly work. When management actively engages in education, supports security specialists and sends a clear message that security is a strategic priority, this attitude gradually permeates the entire organisation.

The creation of SWOT analyses for organisational self-assessment can provide companies with a clear and effective framework for identifying key areas requiring attention. Furthermore, it can serve as a starting point for the implementation of specific measures and for enhancing security awareness across the organisation.

Operational recommendations derived from the SWOT analyses:

- Introduce mandatory but role-specific cybersecurity training, with short modules for all staff and deeper exercises for high-risk roles.
- Use simulated attacks only with feedback, reflection and follow-up training, and measure both click rates and reporting behaviour.
- Establish internal cybersecurity ambassadors who connect local work practices with central security policies.
- Raise awareness of AI-related threats through scenarios covering deepfakes, voice cloning and social engineering.
- Implement BYOD and secure remote-access rules as part of training, not only as technical or legal documents.
- Foster a cybersecurity culture that rewards early reporting and treats errors as opportunities for organisational learning.

For all the reasons mentioned, it can be concluded that education in the field of cybersecurity is not merely a matter of legal compliance or the fulfilment of formal requirements, but above all a tool for long-term competitiveness. Companies that approach it strategically gain an advantage not only today but also in the future.

11 REFERENCES

[1] Redakcia, *Počet kybernetických útokov na Slovensku v prvom polroku prudko rástol*, NEXTECH 2025. [Online]. Available: https://www.nextech.sk/a/Pocet-kybernetickych-utokov-na-Slovensku-v-prvom-polroku-prudko-rastol

[2] I. Lella, M. Theocharidou, E. Magonara, A. Malatras, R. Svetozarov Naydenov, C. Ciobanu, and G. Chatzichristos, Eds., *ENISA Threat Landscape 2024*, 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[3] ESET, *Školenie kybernetickej bezpečnosti*, 2026. [Online]. Available: https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/riadenie-it-bezpecnosti/skolenie-kybernetickej-bezpecnosti/

[4] IBM, *Cost of a Data Breach Report 2025*, 2025 [Online]. Available: https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

[5] Národný bezpečnostný úrad SR, *Upozornenie na AI model*, 2025. [Online]. Available: https://www.nbu.gov.sk/upozornenie-na-ai-model/

[6] IBM, *Cost of Data Breach Report 2023*, 2023. [Online]. Available: https://thehackernews.com/2023/12/cost-of-data-breach-report-2023.html

[7] ISACA, *ISACA Journal, Volume 5, 2022*. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5

[8] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," *Computers & Security*, vol. 136, p. 103585, 2024. https://doi.org/10.1016/j.cose.2023.103585

[9] D. Hillman, M. Hennessy, and C. B. Mayhorn, "Evaluating organizational phishing awareness training on an enterprise scale," *Computers & Security*, vol. 134, p. 103461, 2023. https://doi.org/10.1016/j.cose.2023.103461

[10] A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring cybersecurity education and training techniques: A systematic review," *Symmetry*, vol. 15, no. 12, p. 2175, 2023. https://doi.org/10.3390/sym15122175

[11] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, "Workforce framework for cybersecurity (NICE framework)," NIST Special Publication 800-181 Revision 1, National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-181r1

[12] G. Ho *et al.*, "Understanding the efficacy of phishing training in practice," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2025. https://doi.org/10.1109/SP61157.2025.00076

[13] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: Defining gamification," in *Proceedings of the 15th International Academic MindTrek Conference*, 2011, pp. 9–15. https://doi.org/10.1145/2181037.2181040

[14] N. H. Weeratunge *et al.*, "Game-based cybersecurity awareness and education: A scoping review," *Information Systems Frontiers*, 2026. https://doi.org/10.1007/s10207-026-01239-9

[15] PwC, *2022 Global Risk Survey*, 2022. [Online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-global-risk-survey-report-2022-main.pdf

[16] GDPR – General Data Protection Regulation.

[17] NIS2 – Directive (EU) 2022/2555.

[18] Denisa Šukolová, *Kontexty andragogického výskumu*. Bratislava: Národný inštitút vzdelávania a mládeže, 2019. [Online]. Available: https://www.researchgate.net/publication/338535965_KONTEXTY_ANDRAGOGICKEHO_VYSKUMU

[19] V. Tamášová, J. Péteriová, and S. Barnová, "Nové výzvy a trendy v andragogickej profesionalizácii študentov andragogiky na Slovensku," ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/327766191_Nove_vyzvy_a_trendy_v_andragogickej_profesionalizacii_studentov_andragogiky_na_Slovensku

[20] Y.-M. Lee, "Mobile microlearning: A systematic literature review and its implications," *Interactive Learning Environments*, vol. 31, no. 7, pp. 4636–4651, 2023. https://doi.org/10.1080/10494820.2021.1977964

[21] S. Balasundaram, J. Mathew, and S. Nair, "Microlearning and learning performance in higher education: A post-test control group study," *Journal of Learning for Development*, vol. 11, no. 1, pp. 1–14, 2024. [Online]. Available: https://files.eric.ed.gov/fulltext/EJ1423546.pdf

[22] J. Stebila, "Rozvoj inovatívnych foriem vzdelávania. Didaktika odborného výcviku," Banská Bystrica: Univerzita Mateja Bela, n.d. [Online]. Available: https://lms.umb.sk/mod/resource/view.php?id=38624

[23] E. Wenger, *Communities of Practice: Learning, Meaning, and Identity*. Cambridge: Cambridge University Press, 1998. https://doi.org/10.1017/CBO9780511803932

[24] SURF, "Blended education explained," n.d. [Online]. Available: https://www.surf.nl/en/themes/blended-education/blended-education-explained

[25] M. Púpavová, "Gamifikácia a eLearning vo vzdelávaní: Čo tieto pojmy znamenajú?" *Eduworld*. [Online]. Available: https://eduworld.sk/cd/martina-pupavova/2170/gamifikacia-a-elearning-vo-vzdelavani-co-tieto-pojmy-znamenaju

[26] S. Tesaříková, "Gamifikace výuky kybernetické bezpečnosti za využití CTF platforem," 2021. [Online]. Available: https://theses.cz/id/uwx32r/

[27] R. Machová, F. Lilla, Z. Godany, and E. Korcsmáros, "Gamifikácia a vzdelávanie manažérov – Inovatívne metódy vo vzdelávaní v teórii a praxi," ResearchGate, 2020. [Online]. Available: https://www.researchgate.net/publication/354294716_Gamifikacia_a_vzdelavanie_manazerov_-_Inovativne_metody_vo_vzdelavani_v_teorii_a_praxi

[28] V. Koutroubas and M. Galanakis, "Bandura's social learning theory and its importance in the organizational psychology context," *Psychology Research*, vol. 12, no. 6, pp. 315–322, 2022. https://doi.org/10.17265/2159-5542/2022.06.001

[29] S. McLeod, "Albert bandura's social learning theory," SimplyPsychology, 2025. [Online]. Available: https://www.simplypsychology.org/bandura.html (cit. 14.9.2025).

[30] B. Halúsková and E. Mošková, "Využívanie technológií v oblasti vzdelávania v bezpečnosti," Zlín: UTB, 2022. [Online]. Available: https://trilobit.fai.utb.cz/Data/Articles/PDF/f28a8f78-693b-439d-989e-a104780e8925.pdf (cit. 14.9.2025).

[31] L. Hofreiter, "Security culture and security management," *Krízový Manažment*, vol. 14, no. 2, pp. 63–68, 2015. https://doi.org/10.26552/krm.C.2015.2.63-68

[32] S. Heseková, "Problematika ESG na finančných trhoch," Zenodo, 2023. [Online]. Available: https://doi.org/10.33542/VSCD-0269-5-07

[33] Slov-lex. Zákon č. 69/2018 Z. z. [Online]. Available: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

[34] Slov-lex. Zákon č. 366/2024 Z. z. [Online]. Available: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/

[35] Slov-lex. Zákon č. 226/2025 Z. z. [Online]. Available: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/226/vyhlasene_znenie

[36] Slov-lex. Zákon č. 227/2025 Z. z. [Online]. Available: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/227/vyhlasene_znenie

[37] EUR-Lex. Directive (EU) 2022/2555 of the European Parliament and of the Council. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

12 AUTHORS

Pavel Beňo is currently working at Comenius University in Bratislava and at Trnava University in Trnava, has a Ph.D. from the Faculty of Applied Informatics at Tomas Bata University in Zlín, Czech Republic, in the fields of remote laboratories, security and cloud computing. He is a research assistant and creator of the cloud computing technology for university and REMLABNET purposes. He is also an expert in network security and penetration testing in computer crime prevention. He is the author of many publications in the field of informatics, security and education. For many years he has worked as a teacher with research in pedagogy and didactics of the sciences (E-mail: pavel.beno@uniba.sk).

Roman Hrmo is a Professor at the Department of Didactics of Vocational Subjects at DTI University, Slovakia. A leading expert in engineering pedagogy, he serves on the doctoral council for Didactics of Technical Subjects. He has contributed to internationally recognised research and led multiple scientific projects. He holds memberships in key bodies, including the Executive of IGIP and the EUR-ACE® Label Committee of ENAEE, and serves as President of the Slovak Monitoring Committee of IGIP (E-mail: hrmo@dti.sk).