[1.] Zoltán SEBÁN, [1.] Róza SZÁMADÓ

CYBER–AWARENESS: PERSONAL OR ORGANIZATIONAL ISSUE?

[1.] Obuda University, Doctoral School on Safety and Security Sciences, Budapest, HUNGARY

Abstract: The study examines cyber awareness and the possibilities of awareness–raising from the perspective of trainers, in the context of individual responsibility and organisational culture. It presents the European Union's current regulatory framework, with particular emphasis on the NIS2 Directive, which conceptualises cybersecurity not only as a technological issue, but also as an organisational and human one. The research is based on a qualitative methodology, drawing on thematic analysis of semi–structured interviews with ten experts engaged in cyber and information security training. The findings indicate that expert narratives strongly foreground the human factor and tend to individualise risk, while organisational processes, resources and cultural patterns are often pushed into the background. The ideal type of the "good" employee is characterised by high–level cognitive, attitudinal and technical expectations, for which organisations frequently fail to provide adequate conditions. The study argues that the development of cyber awareness can only be sustainable and effective if training interventions are closely aligned with organisational culture, leadership commitment and the structures of everyday work.
Keywords: cybersecurity, cybersecurity awareness, organizational culture, NIS2 compliance, raising awareness

1. INTRODUCTION

Cybersecurity has become a central topic among security threats over the past decade. The fundamental reason is that state operations, economic processes, public services and social communication increasingly rely on network and information systems, so their vulnerabilities now pose not only technical, but also operational, legal and strategic risks (European Commission, 2024; NIS2 Directive). The European Union's regulatory approach is based on the premise that cybersecurity is a shared resilience issue across the entire Union, which cannot be limited exclusively to technical protective measures, but also encompasses organisational, leadership and human components (European Commission, 2024; NIS2 Directive).

The results presented in this study are partial findings of a research project aimed at examining cyber and information security awareness, as well as assessing the possibilities, instruments and effectiveness of awareness-raising. The research focuses on the organisational, managerial and human components mentioned above, mapping the current situation and exploring future options for organisational and individual cyber awareness-raising.

2. CYBERSECURITY: PROBLEM AND SIGNIFICANCE

Cybersecurity is no longer merely a technical speciality, but a fundamental precondition of modern state and economic functioning, having become one of the central dimensions of managing national security, economic and societal risks (Kassai, 2024). The phenomena associated with cyberspace are in constant and rapid flux, which requires states, governmental bodies, and social and economic actors to adapt to the dynamic evolution of threats, vulnerabilities and security requirements (Kassai, 2024). According to the European Commission, cybersecurity constitutes a prerequisite for the operation of the digital single market, since without the reliability of network and information systems neither the continuity of critical infrastructures nor citizens' trust in digital services can be ensured (European Commission, 2024). The significance of cybersecurity is therefore twofold: on the one hand, it is linked to the prevention of direct operational and financial damage caused by cyberattacks, and on the other, to the protection of social trust, the rule of law and democratic processes (European Court of Auditors, 2022; Kassai, 2024).

In recent years, the number and complexity of cyberattacks have risen steeply, as confirmed by both national and international statistics. According to Dániel Berzsenyi, the increase in incidents occurring in cyberspace is partly attributable to the expanding attack surface associated with the spread of information and communication technologies, and partly to underfunding, a lack of awareness and the systematic underestimation of exposure (Berzsenyi, 2017). Reports by the European Union Agency for Cybersecurity (hereinafter: ENISA) and other Union bodies indicate that the proportion of incidents affecting critical sectors is particularly alarming, as their consequences may lead to systemic operational disruptions, supply-chain disturbances and

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

security-policy tensions (ENISA, 2023; European Commission, 2024). During the COVID-19 pandemic, the rapid expansion of teleworking, cloud-based services and online administration created additional exposure, resulting in the emergence of new attack vectors and the generalisation of threats that had previously appeared in a narrower context (Selján, 2021).
Current cybersecurity challenges manifest themselves in several interrelated dimensions. On the one hand, the technological complexity of threats is increasing: advanced persistent threats, ransomware campaigns, supply-chain attacks and artificial-intelligence-based attack techniques are bringing to the surface new types of vulnerabilities (Kassai, 2024; European Commission, 2024). On the other hand, the human and organisational challenges of cybersecurity – such as shortages of skilled professionals, low levels of security awareness, and resistance or indifference embedded in organisational cultures – hamper the effective implementation of regulatory and technical measures (Berzsenyi, 2017; Hu et al., 2012). The European Court of Auditors points out that the implementation of the Union's cybersecurity policy is further complicated by the multitude of institutional actors, differences in transposition among Member States and the unequal distribution of resources, which in practice may create an "implementation gap" between declared objectives and actual defensive capabilities (European Court of Auditors, 2022).

3. THE LAYERS OF CYBERSECURITY AND THE HUMAN DIMENSION

The cybersecurity literature and practical frameworks frequently conceptualise protection as a layered system in which physical infrastructure, network, application and data layers, as well as the user environment, constitute interrelated yet distinguishable dimensions. The essence of this approach is that the effectiveness of defence does not depend on a single technical control, but on the coordination and mutual reinforcement of the various defensive layers (Nieles et al., 2017; ENISA, 2015). Within this understanding, the human layer occupies a distinct position, as it appears simultaneously as a vulnerability and as a resource: user behaviour, decision-making routines, attention, trust and organisational norms determine how technical and regulatory controls are realised in everyday operations (Gyaraki, 2022; Nemzeti Kibervédelmi Intézet, 2019; Berzsenyi, 2017).
The human-centred cybersecurity perspective rests on the premise that secure operation cannot be achieved solely through technological solutions and compliance obligations; rather, the specificities of human information processing, the context of user decisions and the supportive or obstructive role of the organisational environment must also be taken into account. From this standpoint, security systems must not only protect the user, but must be designed in such a way that they actively support secure behaviour, reduce opportunities for error and enable users to become active agents of defence (Zimmermann & Renaud, 2019). The principle of user-centred, usable security has therefore become a shared conceptual framework for technological design, awareness-raising and organisational practices (Kelley et al., 2023; Zimmermann & Renaud, 2019).
Within the interpretation of the human dimension of cybersecurity, two distinct approaches can be differentiated. The "human-as-problem" perspective portrays the user primarily as a source of risk – an error-prone, manipulable actor who must be compensated for through rules, sanctions and technical controls (Zimmermann & Renaud, 2019). In contrast, the "human-as-solution" approach emphasises that humans are not only sources of vulnerability, but can also be developable security resources, provided that the organisation supplies appropriate knowledge, feedback, motivation and a supportive culture (Zimmermann & Renaud, 2019; Kelley et al., 2023).
The difference between these two perspectives is not merely of theoretical relevance; it has direct implications for whether organisations conceptualise cyber awareness-raising as a restrictive, control-oriented practice or as a developmental, participatory process. The Figure 1 below illustrates the contrast between these two interpretations.

4. CYBERSECURITY AND CYBER AWARENESS: REGULATORY FRAMEWORKS

In the European Union, the current fundamental framework for cybersecurity obligations is laid down in Directive (EU) 2022/2555 of the European Parliament and of the Council (hereinafter: NIS2 Directive). The aim of the Directive is to establish a uniformly high level of cybersecurity across the entire Union and, to this end, it introduces a broader personal and sectoral scope, clearer rules and stronger supervisory and enforcement mechanisms than the preceding NIS1 framework (European Commission, 2024; NIS2 Directive). According to the Commission's summary, NIS2 covers eighteen critical sectors and requires Member States to develop national cybersecurity strategies, enhance their cybersecurity capabilities and ensure cross-border cooperation (European Commission, 2024). NIS2 imposes several interrelated obligations on the entities

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

concerned. These include cybersecurity risk-management measures, obligations relating to the handling and reporting of incidents, solutions supporting business continuity, consideration of supply-chain security, as well as the explicit allocation of management responsibilities (NIS2 Directive, 2022, arts. 20-23; European Commission, 2024).

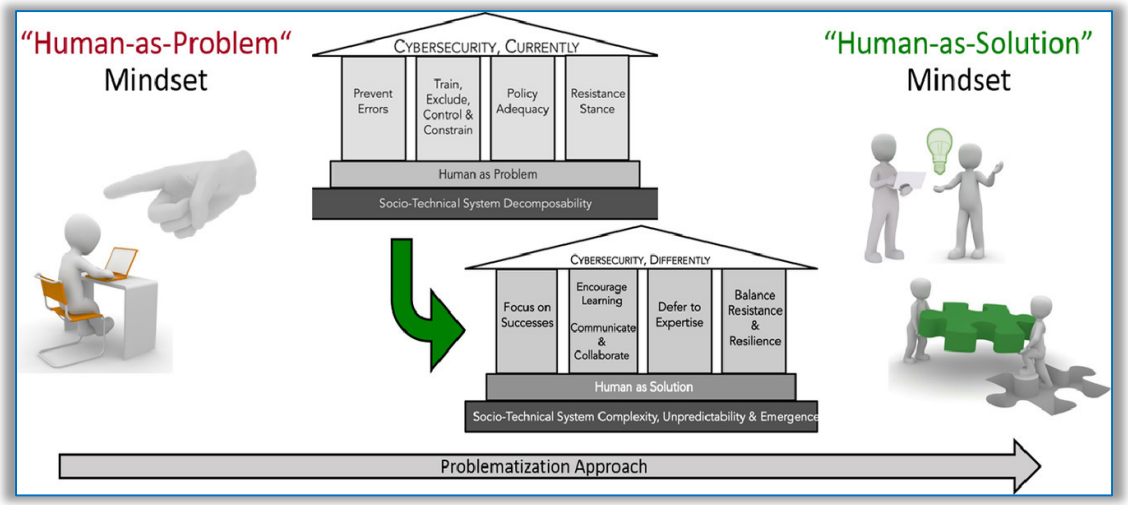

Figure 1. The Mindset of „Human–as–Problem" vs. „Human–as–Solution"
(Adapted from Zimmermann & Renaud, 2019)

It is particularly significant that the Directive establishes accountability at the level of governing bodies, meaning that cybersecurity is no longer merely an IT or operational matter, but becomes an integral part of corporate governance and compliance (NIS2 Directive, art. 20). At the same time, the regulation emphasises the role of cybersecurity education and awareness, as national strategies must address education, awareness-raising and skills development (NIS2 Directive, art. 7; European Commission, 2024).

As is evident from the provisions of NIS2, the human factor plays a decisive role in cybersecurity. Hungarian literature highlights that users' behaviour, level of knowledge, routines and risk perception directly influence the degree of organisational vulnerability; therefore, the human being is not merely one element of defence, but often its most critical point (Gyaraki, 2022; Nemzeti Kibervédelmi Intézet, 2019). Réka Gyaraki emphasises that the technological environment of the average user changes more rapidly than security-conscious behaviour can become routine, which is why organisations require deliberate development and educational practices (Gyaraki, 2022). The Nemzeti Kibervédelmi Intézet reaches a similar conclusion when, in discussing the psychological aspects of information security, it points out that decision-making, attention, susceptibility to influence and habits significantly shape security risks (Nemzeti Kibervédelmi Intézet, 2019). The human factor is therefore dual in nature: it represents a source of vulnerability, yet at the same time a resource that, through appropriate training, practice and organisational culture, can be transformed into an active component of defence (Gyaraki, 2022; Nemzeti Kibervédelmi Intézet, 2019).

In this context, the concepts of awareness, cyber awareness and cyber awareness-raising are of particular significance. In general terms, awareness means that the individual recognises threats, understands their consequences and is able to make situation-appropriate decisions (Gyaraki, 2022; Nemzeti Kibervédelmi Intézet, 2019). Cyber awareness is the form of this awareness that relates specifically to the digital environment: the user is familiar with the risks present in cyberspace, recognises typical forms of attack and, in everyday activities, adheres to the norms of secure digital behaviour (Gyaraki, 2022; ENISA, 2015). Cyber awareness-raising can be understood as an organised developmental process that, through training, communication, practice and organisational feedback, establishes and maintains this knowledge and behaviour (Gyaraki, 2022; NIS2 Directive, art. 7). The importance of the concept lies in the fact that the effectiveness of cybersecurity does not derive solely from technical controls, but also from the extent to which members of the organisation are able to apply these controls correctly and to identify risks in a timely manner (European Commission, 2024; Nemzeti Kibervédelmi Intézet, 2019).

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

5. PERSONAL AND ORGANIZATIONAL CHARACTERISTICS OF CYBER AWARENESS ACCORDING TO AWARENESS-RAISING TRAINERS

Following the review of literature and previous relevant research, qualitative data collection was carried out in the form of expert interviews, using semi-structured interview guides. The sample consisted of ten experts engaged in cyber and information security who also have experience in delivering training, selected through snowball sampling. The interviewees had heterogeneous backgrounds: the public sector, the private sector, higher education and, in particular, the financial sector were all represented in the sample. All participants had a technical or IT degree, and six of them held a doctoral degree; their professional experience ranged between 7 and 25 years. Data collection took place between March and May 2025, with an average interview duration of approximately 90 minutes. The data were analysed using thematic analysis, which made it possible to identify recurring meaning patterns, narratives and interpretive structures (Braun & Clarke, 2006; Kvale, 2005).

Table 1. Main characteristics of the interviewees

Interview ID	Age (year)	Highest degrees(s)	Employer	Professional experience (year)
1	41	Computer Engineer, Security Engineering Engineer, Engineering Teacher, Public Education Manager, Informatics Teacher	public sector, private sector	20
2	55	Mechanical Engineer, Computer Engineer, Security Engineering Engineer, Postgraduate Programme in Cyber Law	private sector	8
3	57	Computer Engineer, Engineering Teacher	public sector, private sector	20
4	45	Electrical Engineer, PhD in Military Engineering	higher education, private sector	15
5	62	PhD in Military Engineering	higher education	25
6	32	Security Engineering, PhD	private sector	7
7	40	PhD in Military Engineering	higher education, private sector	10
8	39	Business Informatics, PhD in Military Engineering	private sector	10
9	40	PhD in Military Engineering	higher education, private sector	10
10	49	Electronics Technician	private sector	

The synthesised analysis of the interviews shows that the human factor occupies the focal point of the experts' perspective, and that the problem of cyber and information security appears primarily not as an organisational or technological issue, but as a matter of employee and managerial responsibility. The respondents consistently identified the primary sources of vulnerability in user inattention, excessive trust, routine clicking behaviour, low risk perception and susceptibility to manipulation. This interpretation is in line with the "human-as-problem" approach, which portrays the user as the bearer of risk rather than as an active, supportable agent of defence (Zimmermann & Renaud, 2019). At the same time, one of the important scientific contributions of the interviews is that they reveal not only what is explicitly present in the expert narratives, but also what is absent from them: technological infrastructure, processes, work organisation and organisational controls appear only as elements of secondary importance, even though in the relevant literature cybersecurity is conceptualised as a socio-technical system (Nieles et al., 2017; Hu et al., 2012).

One of the most important nodal points of the results is the system of expectations towards employees. On the basis of the interviews, the image of the "reliable" employee emerges as an ideal type who simultaneously possesses alertness, healthy suspicion, critical thinking, rule-compliance, source-verification skills, basic digital literacy and adequate risk-assessment capability. According to the experts' formulations, the desirable employee does not act immediately, checks the original source, recognises phishing attempts, does not allow themselves to be pressured and maintains a continuously reflexive, deliberative relationship with the digital environment in everyday work. Expectations towards employees therefore go beyond mere knowledge of rules: the experts essentially expect a cognitive and moral habitus that enables individuals to interpret information, recognise suspicious situations and postpone decisions. This finding is consistent with research showing that analytical reasoning, critical information processing and a lower reliance on heuristic decision-making can reduce vulnerability to online fraud and phishing attacks (Kelley et al., 2023; Frauenstein et al., 2020).

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

However, this system of expectations is also problematic, because it implicitly places at the centre an employee ideal that is in part detached from the actual human-resource practices of organisations. The interviews hardly address the question of the extent to which organisations seek, during recruitment and selection, those skills and personality traits that may be relevant for cybersecurity reliability. Nor is it often discussed how everyday work organisation, overload, time pressure or poorly designed processes make it difficult for employees to actually meet these expectations. Consequently, one important way of interpreting the interview material is that the cybersecurity responsibility placed on employees is, to some extent, excessive and individualising. If the organisation does not select the right person, does not provide sufficient time for rule-compliance, does not ensure supportive feedback systems and does not establish consistent controls, then responsibility for risk does not lie solely with the individual, but also with the organisation. This insight is in line with the NIST approach, which conceives information security as an integrated management task, as well as with compliance research suggesting that employees' adherence to rules cannot be interpreted merely as a personal trait. (Pascoe et al., 2024; Nieles et al., 2017; Hu et al., 2012).

In the updated NIST Cybersecurity Framework 2.0, this organisational responsibility is made explicit by framing cybersecurity as a governance and risk-management function that must be embedded in structures, roles and decision-making processes, rather than delegated to individual employees in isolation. The framework emphasises that organisational context, leadership commitment and clearly defined responsibilities are key determinants of how effectively the core functions of Identify, Protect, Detect, Respond and Recover can be implemented in practice. Against this background, the figure below, which illustrates the organisational implementation of the NIS/NIST cybersecurity framework, can be read as a visual representation of how responsibility for cyber risk is institutionally distributed, and how individual behaviour is situated within broader organisational structures and processes. (Pascoe et al., 2024)

Figure 2. Steps for creating and using a CSF Organizational Profile
(Adapted from Pascoe et al., 2024)

With regard to the expectations placed on employees, another important feature of the interviews is that experts articulate these expectations not as specialised but as general ones. Critical thinking, digital literacy and suspicion appear as norms that apply not only to certain positions, but practically to all organisational actors. This is particularly noteworthy given that exposure to cybersecurity risks, decision-making autonomy, the depth of information processing and control over resources may in fact differ substantially between roles. Nevertheless, the expert narrative homogenises the employee side: the "good" worker is characterised by the same attitudes and skills everywhere. As a consequence, problems are easily framed as moral or personality deficits, rather than as issues of organisational fit. The literature, however, suggests that the antecedents of proactive information security behaviour are simultaneously cognitive, organisational and contextual; skills, motivation and organisational context jointly shape actual behaviour (Tsohou et al., 2023; Choi et al., 2018).

Another key focal point of the analysis is the role of organisational culture and its partial absence in expert interpretations. The interviews frequently indicate that the formal completion of training, in itself, does not result in lasting attitudinal or behavioural change. Several observations point to the fact that ticking off e-learning courses for administrative purposes, having tests filled out by "proxies", lack of time and the difficulty of releasing employees from work for training all suggest that the organisation does not genuinely consider cybersecurity to be an internal operational value. In such a situation, training becomes an external obligation rather than an internalised norm. Within the present analysis, this is a particularly important finding, as it highlights that the effectiveness of cyber awareness-raising depends not only on methodological creativity, but also on whether the organisation provides a cultural and operational environment in which security can become a natural part of everyday work. The literature on organisational

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

support and organisational identification suggests that employees' rule-compliant and committed behaviour strongly depends on the extent to which they perceive themselves as valued, legitimate and supported members of the organisation (Rhoades & Eisenberger, 2002; Kurtessis et al., 2017; Ashforth & Mael, 1989).

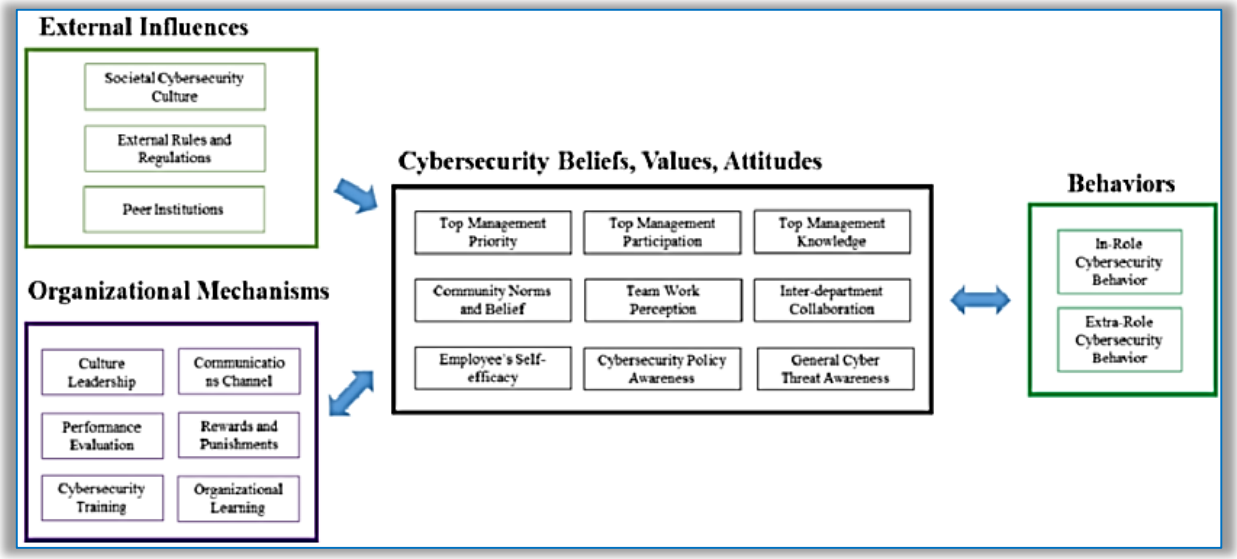

Figure 3. Organizational Cybersecurity Culture Model (Adapted from Huang & Pearlson, 2019)

The importance of organisational culture is also made visible indirectly in the interview material through various forms of resistance. The document repeatedly indicates that it is difficult to make employees feel invested, that time available for training is scarce and that security knowledge often fails to become embedded in daily routines. This implies that cyber awareness is not only a matter of learning, but also a question of organisational psychology and organisational development. If the norm of security does not appear in managerial communication, in process design, in feedback practices and in the system of recognition, then even the best-designed training may easily remain a short-term information-transfer exercise. Organisational culture is therefore not a background factor, but a central condition for the internalisation of knowledge. Karlsson and colleagues (2022) have shown that perceived organisational culture is directly associated with employees' information security compliance, while Hu and co-authors (2012) argue that top management's role and culture jointly shape rule-compliance. Accordingly, the present interview material suggests that the development of cyber awareness can only be sustainable if the organisational embeddedness of training receives at least as much emphasis as its content and methodology.

According to the interviews, the training profession places strong faith in methodological innovation: gamification, simulations, escape-room logic, short digital messages, visual reminders and phishing tests are all presented as solutions that can make awareness-raising more engaging and effective. These solutions can be scientifically justified, as experiential learning, processing tied to practical situations and direct feedback can indeed promote behavioural change. In educational theory approach these tools can be suitable for guiding the learner through each of the levels described in Bloom's taxonomy. The original Bloom's taxonomy named the levels in 1956 as a measure, but in 2001 a revision was made that names the levels by focusing on learner activity and action, as shown in Figure 4 (DeFalco, 2018).

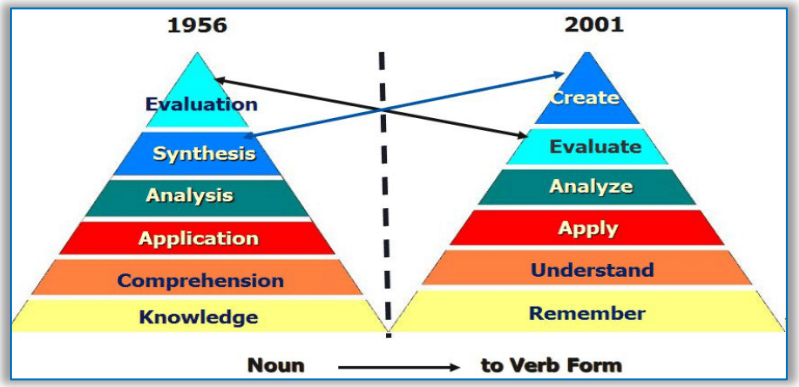

Figure 4. Change of Bloom's Taxonomy from 1956 to 2001 (Adapted from DeFalco, 2018)

All of the technical-methodological tools listed by the experts can be suitable for the learner to acquire knowledge that can be used in practice as an active participant in the new approach to

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

taxonomy. It is important to note that the expert responses, however, indicate that the search for solutions is primarily directed towards technical-methodological tools, with less reflection on the fact that attitudinal resistance, indifference or merely formal compliance are often rooted in organizational cultural factors. Awareness-raising can become a genuine organisational intervention only if it does not merely ask what content should be taught and in what format, but also examines which work processes, leadership examples, time allocations and incentives enable the practical application of what has been learned (Choi et al., 2018; Karlsson et al., 2022).
The significance of organisational culture is further reinforced by the issue of leadership attitude. According to the interviewees' experiences, management is often reactive, and many organisations are only willing to address cybersecurity in earnest once an incident has occurred, when external regulatory pressure arises or when direct economic harm is imminent. The "we will act when something happens" logic, resource constraints and the treatment of security as a necessary evil constitute one of the most important obstructive elements of organisational culture. This mindset represents not only a resource problem, but also conveys a normative message to employees: that security is secondary to productivity, speed or short-term economic interests. Research on organisational behaviour indicates that employees' compliance with rules strongly depends on how visibly and consistently leadership upholds a given norm (Hu et al., 2012). The present findings therefore suggest that cyber awareness cannot be built solely from the bottom up, from the employee side; without leadership legitimacy and organisational prioritisation, awareness-raising is likely to remain a formalised practice with low effectiveness.

6. CONCLUSIONS

Overall, it can be concluded that the growing importance of cyber defence is jointly explained by increasing digital dependence, the strategic revaluation of cyberspace and the tightening of the regulatory environment (European Commission, 2024; NIS2 Directive; Prucková, 2022). The NIS2 Directive makes it clear that cybersecurity is no longer merely a technological issue, but a resilience task grounded in managerial, organisational and human competences (European Parliament and the Council of the European Union, 2022, arts. 7, 20-23). Consequently, the development of cyber awareness and cyber awareness-raising is not a supplementary activity, but one of the basic preconditions of contemporary cybersecurity practice (Gyaraki, 2022; European Commission, 2024; Nemzeti Kibervédelmi Intézet, 2019).
Comparing the findings of the literature with the expert interviews, it can be stated that the cybersecurity requirements imposed on employees and the question of organisational culture cannot be separated from one another. The more complex the set of skills and attitudes an organisation expects from its employees, the more necessary it is for the organisation itself to create the conditions for these expectations to be met: in recruitment and selection, in training, in managerial communication, in work-time organisation, in the design of incentives and in the development of the technical environment. One of the most important lessons of the interview series is therefore that cyber awareness cannot be reduced to the training of individuals. Rather, it can be described as a complex organisational phenomenon in which employee skills, leadership commitment, cultural norms, regulatory pressures and technological conditions jointly shape actual security practices (Hu et al., 2012; Karlsson et al., 2022; Nieles et al., 2017). In the field of cybersecurity and the development of cyber awareness, absolute responsibility cannot be assigned either to the individual or to the organisation; the enhancement of cyber awareness must be reflected both in organisational culture and at the level of individuals.

Acknowledgements

This work is a result of the first author's doctoral research, which is being conducted as part of the PhD program of the Obuda University Doctoral School of Security Sciences. The results presented in the article contribute to the ongoing doctoral dissertation, which aims to examine cyber and information security awareness, assessing the possibilities, tools and effectiveness of awareness–raising.

References

[1] Ashforth, B. E., Mael, F., 1989, Social identity theory and the organization. Academy of Management Review, 14 (1), 20–39.
[2] Berzsenyi, D., 2017, A kiberbiztonság humán oldala. Nemzet és Biztonság, 10(2), 83–101.
[3] Braun, V., Clarke, V., 2006, Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
[4] Choi, S. E., Martins, J. T., Bernik, I., 2018, Information security: Listening to the perspective of organisational insiders. Journal of Information Science, 44(6), 752–767.
[5] DeFalco, J., 2018, Standardizing Metadata Tagging with Pedagogical Identifiers. Conference Paper. 2018 ITS Conference, Montreal, Canada

[6] European Commission, 2024, NIS2 Directive: securing network and information systems. https://digital–strategy.ec.europa.eu/en/policies/nis2–directive (last download: 26th May 2026)
[7] European Court of Auditors, 2022, Challenges to effective EU cybersecurity policy. https://www.eca.europa.eu/lists/
[8] European Parliament and the Council of the European Union, 2022, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[9] European Union Agency for Network and Information Security (ENISA), 2015, Definition of cybersecurity: Gaps and overlaps in standardisation (Version 1.0). https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf
[10] European Union Agency for Network and Information Security (ENISA), Report on Cyber Crisis Cooperation and Management. https://www.enisa.europa.eu/publications/report–on–cyber–crisis–cooperation–and–management
[11] Frauenstein, E. D., Flowerday, S. V., Furnell, S. M., 2020, Susceptibility to phishing on social network sites: A personality information processing model. Computers & Security, 94, 101862.
[12] Gyaraki, R., 2022, A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról. Magyar Rendészet, 22(2), 245–261.
[13] Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012, Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660.
[14] Huang, K., Pearlson, K., 2019, For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In Tung Bui, editor, 52nd Hawaii International Conference on System Sciences, HICSS 2019, Grand Wailea, Maui, Hawaii, USA. pages 1–10, ScholarSpace
[15] Karlsson, M., Karlsson, F., Åström, J., Denk, T., 2022, The effect of perceived organizational culture on employees' information security compliance. Information & Computer Security, 30(3), 382–401.
[16] Kassai, Z., 2024, A jelen kiberbiztonsági fenyegetései és a jövő kihívásai. Hadtudományi Szemle / Hadmérnök, 19(1), 121–141.
[17] Kelley, N. J., Hurley–Wallace, A. L., Warner, K. L., Hanoch, Y., 2023, Analytical reasoning reduces internet fraud susceptibility. Computers in Human Behavior, 142, 107648.
[18] Kurtessis, J. N., Eisenberger, R., Ford, M. T., Buffardi, L. C., Stewart, K. A., Adis, C. S., 2017, Perceived organizational support: A meta–analytic evaluation of organizational support theory. Journal of Management, 43(6), 1854–1884
[19] Kvale, S., 2005, Az interjú: Bevezetés a kvalitatív kutatás interjútechnikáiba. Jószöveg Műhely Kiadó, Budapest.
[20] Nemzeti Kibervédelmi Intézet, 2019, Az információbiztonság lélektana, Budapest.
[21] Nieles, M., Dempsey, K., Pillitteri, V. Y., 2017, An introduction to information security (NIST Special Publication 800–12 Rev. 1). National Institute of Standards and Technology.
[22] Pascoe, C., Quinn, S., Scarfone, K., 2024, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, [online]
[23] Prucková, M., 2022, Cyber attacks and Article 5 – A note on a blurry but consistent position of NATO. NATO Cooperative Cyber Defence Centre of Excellence.
[24] Rhoades, L., Eisenberger, R., 2002, Perceived organizational support: A review of the literature. Journal of Applied Psychology, 87(4), 698–714.
[25] Selján, P., 2021, Kiberbiztonság a koronavírus idején: a COVID–19 nemzetbiztonsági aspektusai. Scientia et Securitas, 2(1), 78–87.
[26] Tsohou, A., Siponen, M., Baltuttis, D., Janson, A., Choi, S. E., 2023, The antecedents of employees' proactive information security behaviors. Information Systems Journal.
[27] Zimmermann, V., Renaud, K., 2019, Moving from a "human–as–problem" to a "human–as–solution" cybersecurity mindset. International Journal of Human–Computer Studies, 131, 169–187.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665