Cyber stress management among employees as part of cybersecurity and psychological resilience in organisations

Aleksander Sapiński[1], Nazar Hlynskyy[2], Jacek Binda[1] and Yanina Lisun[3]

[1]Bielsko-Biala University of Applied Sciences
Poland

[2]Lviv Polytechnic National University
Ukraine

[3]The State University of Trade and Economics
Ukraine

***Abstract*— In the face of a growing number of cyber incidents and the ever-increasing pressure of the digital work environment, the problem of cyber stress is becoming a key factor limiting the effectiveness of an organisation's security strategy. Previous research has focused mainly on technostress analysed from the perspective of individual employee responses, but has overlooked its role in shaping psychological and organisational resilience in the face of cyber threats. This study fills this gap by proposing a new, integrated conceptual model in which cyber stress acts as an intermediary variable between the pressure of the technological environment and the organisation's ability to adapt and recover from incidents. The article contributes three original elements to the literature: (1) it points to the ambivalent nature of cyber stress, which, depending on organisational conditions, can be both destructive and mobilising; (2) it combines the perspective of IT security management with HR policy, emphasising the need to integrate technical procedures with practices that support employee well-being; emphasises the role of safety culture and leadership in transforming digital stress from a risk factor into a resource that strengthens team resilience. In this way, the article expands the state of knowledge in 2024–2025, pointing to directions for further research on a multi-level approach to cyber stress and offering practical recommendations for managers who want to build integrated and resilient safety cultures in the age of digital threats.**

Keywords— cybersecurity management, psychological resilience, digital stress, conceptual management, safety culture

I. EPISTEMOLOGICAL INTRODUCTION

The issue of scientific paradigms in management research plays a fundamental role in explaining organisational phenomena. In the world of science, the commonly accepted foundation is the definition of a paradigm, introduced into the philosophy of science by Thomas Kuhn (1962/2012), which refers to a set of common ontological, epistemological and methodological assumptions that determine how research problems are formulated, methods are selected and results are interpreted. Kuhn emphasised that paradigms are not neutral, but determine the cognitive framework in which researchers perceive 'normal science', and a paradigm shift often means a scientific revolution in which existing explanations are replaced by new ones. In management sciences, the issue of organisational stress, particularly technostress (Tarafdar, Tu, Ragu-Nathan, & Ragu-Nathan, 2007), has been analysed for decades mainly within the positivist paradigm. In this approach, researchers assumed that stress is a measurable, objective psychological phenomenon that can be quantified using psychometric tools. The positivist paradigm stems from the assumptions of ontological realism and epistemological objectivism (Burrell & Morgan, 1979), treating organisations as research objects that exist independently of the observer.

In research on technostress, adopting this paradigm meant focusing on identifying 'stressors' (technostress creators) and their impact on dependent variables such as job satisfaction, productivity, and turnover (Ayyagari, Grover, & Purvis, 2011). In this sense, the positivist paradigm enabled the operationalisation of the phenomenon and its standardised study on large samples of employees, which resulted in the

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 29, No 4 (2025), pages 9
https://doi.org/10.19192/wsfip.sj4.2025.17
Received: May 2025 Accepted: December 2025
Published: December 2025

creation of numerous scales and empirical models (Tarafdar, Pullins, & Ragu-Nathan, 2015). However, in the context of cybersecurity and psychological resilience, the positivist approach faces significant limitations that prevent further use of this paradigm. This is because positivism focuses on linear cause-and-effect relationships, while digital stress in complex and high-risk environments is dynamic and emergent in nature (Sonnentag & Frese, 2013). The reductionist approach to stress as a psychometric variable overlooks broader social and cultural contexts that can significantly modulate the perception and effects of digital stressors (Salanova, Llorens, & Cifre, 2013). Furthermore, the positivist paradigm fits into the logic of control and prediction, and thus remains close to the logic of risk management, but does not fully address the challenges of organisational resilience, which assumes adaptability and learning (Hollnagel, Woods, & Leveson, 2006).

An alternative to the dominance of the positivist approach in research on digital stress and organisational resilience is the interpretive-constructivist paradigm. It is based on the assumption that organisational reality does not exist in an objective and independent way, but is socially constructed in the process of interaction between individuals and groups (Berger & Luckmann, 1966/1991). This means that phenomena such as digital stress, safety culture, and psychological resilience of employees are not only measurable variables, but above all meaningful experiences that acquire meaning through discourse, symbolism, and everyday practices. Unlike positivism, which seeks universal regularities and strives for prediction, interpretivism focuses on understanding (Verstehen) the subjective meanings attributed to situations by organisational actors (Weber, 1978). In research on digital stress, this means paying attention to how employees interpret technologies, how they construct narratives about information overload, and how they negotiate the meaning of security practices within teams. For example, for one employee, the requirement for two-factor authentication may be seen as an expression of the organisation's concern for data, while for another, it may be seen as a symbol of mistrust and an additional source of frustration.

The constructivist perspective allows us to capture these differences and the multitude of interpretations. Research conducted within this paradigm emphasises that digital technologies are not neutral tools, but active elements of the social context that shape everyday work (Orlikowski, 1992; Orlikowski & Scott, 2008). Hence, digital stress cannot be understood solely as an excess of information stimuli, but as the result of a process in which individuals give meaning to their relationships with technology.

The application of the interpretive paradigm in cyber resilience management research also reveals the importance of language and discourse in shaping security culture. Narrative analyses show that employees often internalise or contest official security strategies through stories and metaphors that reflect their own experiences (Vaara, Sonenshein, & Boje, 2016). This approach broadens the understanding of digital stress as a phenomenon rooted in organisational culture, rather than merely as an individual's response to specific technological stressors. The constructivist approach also allows us to see that psychological and organisational resilience is not only based on individual resources or safety procedures, but is co-created through communication practices, team rituals and shared interpretations of crisis situations (Lengnick-Hall, Beck, & Lengnick-Hall, 2011). From this perspective, 'cyber stress management' is not just the implementation of protective tools, but a process of building narratives that give meaning to threats and strengthen group cohesion.

However, the interpretive paradigm has its limitations. Critics point out that epistemological relativism makes it difficult to develop universal guidelines for management practice (Alvesson & Deetz, 2000). The inability to generalise the results of qualitative research, typical of interpretivism, can be a barrier in a context where decision-makers expect clear, quantitative indicators of the effectiveness of security strategies. However, it is interpretivism that allows us to discover hidden aspects of digital stress that are not accessible to positivist measurement, such as fear of evaluation, feelings of alienation, or ambivalent emotions towards security systems.

From the point of view of the epistemology of cyber resilience research, interpretivism thus provides a critical complement to positivism. Where positivism provides us with knowledge about what is happening (e.g., an increase in burnout rates as a result of information overload), interpretivism allows us to understand how and why employees attach meaning to these phenomena. In other words, instead of seeking universal laws, interpretivism seeks to reveal the richness of experiences and meanings that constitute organisational life.

Recent studies highlight the important — but still fragmentarily addressed — links between stress related to cyber threats and employee well-being and effectiveness. For example, an SEM analysis conducted by 'Digital detox...' (Mizrak et all. 2025) showed that cyber security fatigue significantly impairs productivity and mental health, and that support in the form of a 'digital detox' mitigates these negative effects. A Grounded Theory-based study in financial institutions (Farheen et all. 2024) identifies core mechanisms of psychological resilience among cybersecurity professionals — such as communication protocols and systemic support — that remain insufficiently integrated into current protective action models.

At the same time, research on Zero Trust architecture (2025) shows that technical security systems can unduly restrict social trust and hinder collaboration — pointing to the need for a synergistic perspective that combines technical rigour with cultural sensitivity.

II. CYBER STRESS AS AN INTERMEDIATE VARIABLE

The term 'cyberstress', which is increasingly appearing in management literature, organisational psychology and information security research, is an extension and refinement of the category of 'technostress' introduced by Craig Brod (1984). In the classic approach, it was called technostress and defined

as an ‘adaptive disorder’ of an individual resulting from an inability to cope with the demands of modern computer technology. Initially, this problem was seen rather as an individual challenge related to user competencies and limitations of their adaptive abilities (Brod, 1984). However, with the spread of information and communication technologies, and later digital tools and cloud platforms, the scope of the phenomenon has expanded significantly. Today, cyber stress encompasses issues such as information overload, anxiety related to cyber threats, lack of security, and pressure to be permanently available online (Tarafdar, Pullins, & Ragu-Nathan, 2015; Ayyagari, Grover, & Purvis, 2011). Significantly, there are clear differences in the literature in terms of how this phenomenon is defined and conceptualised, depending on the research paradigm adopted. Researchers rooted in the positivist tradition tend to view cyberstress in terms of a psychometric variable, measurable using questionnaires and standardised assessment tools (Tarafdar et al., 2007; Maier, Laumer, Eckhardt, & Weitzel, 2019). In this approach, cyberstress is treated as an objective factor influencing job satisfaction, productivity, or the level of errors in employee behaviour. In contrast, interpretive-constructivist researchers emphasise the subjective nature of cyberstress, pointing out that it is not a simple function of exposure to technology, but rather the result of individual interpretations, perceptions and meaning-making processes (Day, Scott, & Kelloway, 2010; Stich, Tarafdar, Cooper, & Stacey, 2019). Particularly interesting is the critical view that treats cyber stress as a phenomenon embedded in broader structures of power and organisational control. From this perspective, cyberstress is not merely an individual adaptation problem, but a mechanism of discipline and control in digital work environments, where monitoring tools, reporting systems, and security procedures can be perceived as a form of ‘digital panopticon’ (Zuboff, 2019; Introna, 2016). Researchers in this field point out that cyberstress is not so much a result of technology itself as it is of the ways in which it is implemented, cultural norms, and management policies that enforce constant readiness and control.

In organisational psychology, cyber stress is currently located at the intersection of several key theories of stress and employee well-being. It is worth referring, among others, to the classic transactional stress model of Lazarus and Folkman (1984), in which the process of cognitive assessment of stressors and available coping resources plays an important role. In the context of cyber stress, this means that two people working in the same technological environment may experience completely different levels of stress, depending on their previous experiences, self-assessment of digital competence, or the support they receive from the organisation (Ragu-Nathan, Tarafdar, Ragu-Nathan, & Tu, 2008). Furthermore, an increasing number of studies point to the ambiguous nature of cyber stress – on the one hand, it is a source of risk for burnout, absenteeism and errors (Salanova, Llorens, & Cifre, 2013; Shu, Tu, & Wang, 2011), and on the other, it can be a catalyst for learning and strengthening competencies if the organisation provides adequate resources and support mechanisms (Cooper, Flint-Taylor, & Pearn, 2013). This ambivalence is well illustrated by the research of Tarafdar and co-authors (2015), who showed that some dimensions of technostress – e.g. the feeling of excessive pace of change – can lead to mobilisation and increased innovation, as long as the employee does not experience chronic overload. In past decade, research on cyber stress in the context of information security and cyber threats has gained particular importance. D'Arcy, Herath and Shoss (2014) pointed out that information security requirements, such as complex login procedures or the need for multi-step authorisation, are sometimes perceived as technological stressors, which can lead to strategies of avoidance or circumvention of procedures. This phenomenon, often referred to as ‘shadow security,’ is particularly dangerous because employees may take actions to reduce stress that weaken the actual level of system protection (Bada, Sasse, & Nurse, 2019).

Cyberstress in literature appears not as a one-dimensional psychological phenomenon, but as a multidimensional and multi-paradigmatic category(ENISA 2025). Its definition and conceptualisation depend largely on the research paradigm adopted: positivist (a measurable psychometric construct), interpretative (a subjectively constructed experience) or critical (a tool for organisational control and the reproduction of power). This multidimensionality therefore requires the adoption of an integrated framework that takes into account both the individual dimension (emotions, perception, coping) and the organisational dimension (security policies, work culture, power structures).

III. CYBER STRESS IN ORGANISATIONAL RESILIENCE MODELS

In the literature on the subject, cyber stress is increasingly analysed not only in terms of individual adaptive responses, but also in the broader context of psychological resilience and organisational resilience. As early as the 1980s, stress psychology researchers, including Kobasa (1979), pointed out that not only the intensity of the stressor plays a key role in coping with stress, but also personal resources such as a sense of control, commitment, and treating challenges as opportunities for growth. Contemporary research on cyberstress builds on this tradition, adapting the concept of ‘hardiness’ and salutogenic models (Antonovsky, 1987) to the digital environment. One of the significant turning points in research on psychological resilience was the shift in emphasis from a deficit approach (stress as a destructive factor) to a resource approach (stress as a potential catalyst for development). In this sense, cyberstress can be viewed both as a risk factor leading to burnout and as a challenge that, with the right support, can strengthen employees' adaptive abilities. This logic is well reflected in the Job Demands–Resources Model (Bakker & Demerouti, 2007), in which cyberstress falls into the category of job demands, and psychological resilience is a key job resource that cushions its negative effects. Empirical research confirms that employees with higher levels of psychological resilience are less susceptible to the negative effects of information overload or constant online availability

(Korunka & Vitouch, 2017; Tugade & Fredrickson, 2004).

From an organisational perspective, cyber stress should be treated as part of a broader ecosystem of stressors that can undermine or strengthen the resilience of socio-technical systems. The concept of organisational resilience stems from research on critical systems safety and reliability engineering (Hollnagel, Woods, & Leveson, 2006; Woods, 2015). In this context, resilience is defined as an organisation's ability to 'anticipate, monitor, respond and learn' (Hollnagel, 2011). Cyber stress in this sense is not just an individual problem, but an indicator of an organisation's ability to adapt to dynamic technological changes and growing cyber threats. If an organisation can effectively manage digital stressors – e.g. by designing intuitive security procedures, providing training and supporting employees in the area of digital competences – then cyber stress becomes part of the organisation's learning mechanism, rather than just a burden (Bhamra, Dani, & Burnard, 2011). The debate in the literature revolves around the question of whether psychological and organisational resilience should be treated as a trait (a relatively stable resource) or as a dynamic process. The trait approach (Connor & Davidson, 2003; Block & Kremen, 1996) suggests that some employees are inherently more resilient to stress, which implies the need to select and recruit 'psychologically resilient' individuals for environments with high levels of technological stress. In contrast, the process approach (Luthar, Cicchetti, & Becker, 2000; Fletcher & Sarkar, 2013) emphasises the possibility of developing resilience through management practices, organisational culture and investment in social capital. In the latter view, cyber stress is not only a threat, but also an opportunity to exercise and strengthen adaptive abilities at both the individual and team levels. The debate in the literature revolves around the question of whether psychological and organisational resilience should be treated as a trait (a relatively stable resource) or as a dynamic process. The trait approach (Connor & Davidson, 2003; Block & Kremen, 1996) suggests that some employees are inherently more resilient to stress, which implies the need to select and recruit 'psychologically resilient' individuals for environments with high levels of technological stress. In contrast, the process approach (Luthar, Cicchetti, & Becker, 2000; Fletcher & Sarkar, 2013) emphasises the possibility of developing resilience through management practices, organisational culture and investment in social capital. In the latter approach, cyber stress is not only a threat, but also an opportunity to exercise and strengthen adaptive abilities at both the individual and team levels(Skeoch 2024) . Of particular note is research on team resilience, which indicates that coping with cyber stress together is a function of the quality of communication, trust, and the ability to learn collectively (Alliger, Cerasoli, Tannenbaum, & Vessey, 2015; Meneghel, Salanova, & Martínez, 2016). Teams that develop mechanisms to support each other in situations of digital overload show greater resilience to security incidents and recover more quickly after cyberattacks.

It can therefore be concluded that cyber stress should not be analysed in isolation as an individual psychological problem, but as a phenomenon embedded in complex relationships between the individual and the organisation. Models of psychological and organisational resilience indicate that effective cyber stress management requires integrating the individual perspective (coping, personal resources) with the organisational perspective (procedures, culture, security systems). Only such an approach allows us to move from diagnosing the problem to building organisational systems capable of adapting to permanent digital challenges.

IV. Safety culture and cyber stress

In organisational safety management literature, the concept of safety culture plays a key role in explaining why some organisations cope with threats better than others, despite similar technologies and formal structures. This concept was first widely popularised after the Chernobyl disaster, where reports indicated that the lack of an adequate safety culture – understood as a set of shared values, beliefs and practices – was a critical factor in the escalation of risk (INSAG, 1986). In the following decades, research in aviation, nuclear energy and the medical sector confirmed that it is safety culture, and not just technology or regulations, that determines the effectiveness of risk management (Reason, 1997; Guldenmund, 2000; Antonsen, 2009). In the context of the digital environment, security culture is taking on a new dimension, combining the traditional approach to security with challenges specific to cyberspace. Cyber stress, as a chronic burden on employees resulting from cybersecurity requirements (e.g., the need to use complex passwords, constant updates, or the risk of phishing incidents), is becoming a barometer of the quality of security culture in an organisation. As Badawy, Dudau and Sasse (2021) point out, excessive security procedures can lead to 'security fatigue,' which weakens employees' motivation to comply with rules. In this sense, security culture is not about maximising control, but about balancing security requirements with the mental well-being of employees.

The main mechanism for buffering the impact of cyber stress is the internalisation of security values. In organisations where the security culture is based on trust, transparency and shared responsibility, employees interpret security requirements not as external constraints, but as part of the common good. Research by Parsons and co-authors (2017) has shown that involving employees in the process of co-creating security policies (e.g., consultations when designing procedures) significantly reduces perceived cyber stress and increases compliance with rules. This means that security culture acts as a mediator between the formal structure of security policies and the experience of everyday digital work. An important aspect of safety culture in the context of cyber stress is the role of leadership. Safety leadership, as described by Clarke (2013), emphasises the importance of leaders in modelling attitudes and creating a climate in which safety issues are an integral part of the organisation's mission, rather than just a regulatory add-on. Leaders who promote open communication and empathy towards issues related to digital overload support the reduction of cyber stress and increase the organisation's ability to learn

from mistakes (Krasikova, Green, & LeBreton, 2013). In this context, leadership is not merely a function of hierarchy, but a process of social culture shaping in which safety and well-being are inextricably linked. It can be said that, a culture of safety in cyberspace is directly linked to the concept of learning organisations. Research in the field of resilience engineering (Hollnagel, 2011; Woods, 2015) indicates that the resilience of a system depends on its ability to learn reflectively after incidents and to anticipate potential threats. In a digital environment, where threats are dynamic and often unpredictable, a culture of security enables the conversion of cyber stress experience into an organisational resource: stressors become an impetus for improving procedures and increasing awareness of threats. This means that cyber stress, instead of undermining the effectiveness of an organisation, can be transformed into an element that supports its adaptability – provided that the security culture is open to innovation and learning.

However, the literature also points to the dark side of safety culture. In organisations where safety culture takes the form of a 'blame culture', cyber stress intensifies and employees hide mistakes instead of reporting them (Dekker, 2016). This effect leads to a paradoxical situation: the more emphasis is placed on safety through restrictive controls and sanctions, the greater the risk of violations resulting from defensive behaviour and 'silent resistance'. In contrast, in organisations with a 'just culture' (Reason, 1997) – i.e. a culture of fair treatment of mistakes – cyber stress can be minimised by viewing incidents as opportunities for development and improvement of systems, rather than as excuses for repression.

At this stage, it should be strongly emphasised that safety culture acts as a buffer against cyber stress because it sets the interpretative framework within which employees experience digital safety requirements. Concluding that this culture is based on trust, shared responsibility and learning, cyber stress can be transformed into a source of organisational resilience. However, if the logic of control and punishment prevails, cyber stress becomes a factor that erodes not only the well-being of employees, but also the effectiveness of the entire cybersecurity strategy. This ambivalence points to the need to integrate IT security management with HRM policy.

V. THE THEORETICAL CONCEPT OF THE RELATIONSHIP BETWEEN CYBER STRESS AND ORGANISATIONAL RESILIENCE - METHODOLOGICAL IMPLICATIONS OUTLINE

The construction of a conceptual model is a key stage in any theoretical work in management sciences, as it enables the integration of scattered research approaches into a single analytical structure suitable for further operationalisation. In this study, the proposed model is based on the cognitive-behavioural paradigm, whose basic assumption is to treat the reactions of individuals and teams to cyber threats as the result of cognitive interpretation in relation to available resources and institutional conditions (Lazarus & Folkman, 1984; Weick, 1995). This means that cyber stress is neither a simple physiological reaction nor merely a function of technological overload, but rather a dynamic process in which the organisational context plays a key moderating role.

The first key source is excessive technological complexity. Employees forced to operate increasingly complex IT systems experience a phenomenon known as techno-complexity, which reduces their sense of competence and self-efficacy (Ayyagari, Grover & Purvis, 2011). This complexity includes both the multitude of tools and platforms and the need to manage the flow of information across multiple channels simultaneously, which encourages fragmentation of attention and increases the risk of security errors.

The second source is information overload, understood as an excess of digital stimuli exceeding the perceptual capacities of employees. Research shows that information overload not only causes cognitive exhaustion, but also reduces motivation to follow safety procedures (Eppler & Mengis, 2004).

In an organisational environment, this manifests itself, among other things, in the phenomenon of ignoring security alerts or superficially reviewing protocols.

The third stressor is the pressure of constant availability and immediate response (techno-invasion), resulting from the blurring of boundaries between work and private life in the age of mobile technologies. From a management perspective, this means that employees are constantly 'on call', which contributes to chronic stress and increases the risk of burnout (Mazmanian, Orlikowski & Yates, 2013). Another source is security uncertainty. Unlike traditional occupational stressors, cyber stress includes a component of fear of potential data breaches, loss of reputation or regulatory sanctions (D'Arcy, Herath & Shoss, 2014). At the team level, dysfunctional communication and the pressure of shared responsibility for security can be sources of cyber stress. Research indicates that in teams characterised by low social capital and a deficit of trust, cyber stress more often takes a destructive form (Mulki, Jaramillo & Locander, 2006) . Conversely, in psychologically resilient teams, digital stress is often mitigated by peer support and knowledge sharing. The sources of cyber stress are multi-level and multi-dimensional – ranging from technological factors, through psychosocial factors, to cultural and institutional factors. Their analysis provides a better understanding of why cyber stress plays a key mediating role in the proposed model. At the same time, it sets the stage for subsequent subsections, which will discuss coping mechanisms and the role of organisational resilience.

The central element of the model is cyber stress treated as an intermediate variable. Lazarus's research (1999) indicates that stress results from a cognitive appraisal process in which an individual compares situational demands with available resources. In a digital context, this means that cyber stress not only reduces an employee's cognitive ability and motivation, but can also serve as a warning signal, mobilising them to take protective measures.

From a security management perspective, this is a particularly important aspect: organisations should learn to interpret the symptoms of cyber stress as a 'barometer' of the quality of their security systems. If stress symptoms are

widespread, it means that security procedures are too burdensome or that internal communication does not provide clear standards of conduct (Ragu-Nathan et al., 2008). Mechanisms for coping with cyber stress can be considered in terms of three strategies: cognitive, emotional and behavioural. Cognitive strategies include, among others, reinterpreting cyber threats as opportunities to acquire new skills. Emotional strategies involve reducing anxiety through social support – research shows that employees who can count on their colleagues' help in interpreting security messages are much less likely to experience paralysing fear of making mistakes (LePine et al., 2016). Behavioural strategies include participation in training, practice in cyberattack simulations, and developing habits for safe online work.

At the team level, the phenomenon of shared responsibility plays a key role: highly cohesive teams not only distribute security-related tasks more effectively, but also monitor each other's behaviour, minimising the risk of individual errors. Organisational resilience is the end result of the proposed model. Its essence is the ability of an organisation to absorb disruptions, adapt to changing conditions and quickly restore functions after an incident (Hollnagel, 2011). In the research by Lengnick-Hall and colleagues (2011), resilience was described as an emergent feature that cannot be reduced to the sum of individuals' competencies. This means that cyber stress, when managed properly, can strengthen the adaptability of organisational systems rather than weaken them.

The proposed conceptual model requires a research strategy that captures both the measurable effects of digital stress and the interpretive processes through which employees and teams make meaning of digital threats. Therefore, a mixed-methods strategy based on a sequential explanatory model (Creswell & Plano Clark, 2024) will be implemented. In the first stage, quantitative research will be conducted among employees from at least three sectors (e.g., finance, higher education, and public administration) using an expanded version of the technical stress scale (Tarafdar et al., 2019), supplemented with items assessing the constructive dimension (eustress). This will provide data suitable for hierarchical linear modeling (HLM) and multilevel SEM, enabling the identification of cross-level effects of cyberstress on psychological resilience outcomes.

In the second phase, semi-structured interviews will be conducted with IT security managers, human resources specialists, and selected employees from the study sample. Qualitative data will be analyzed using thematic coding and narrative analysis, with a focus on coping strategies, perceptions of security culture, and leadership practices. Integration of quantitative and qualitative findings will be achieved through joint presentations that combine statistical patterns with illustrative narratives, enabling a richer interpretation of the ambivalent role of cyber stress. This approach not only provides methodological triangulation but also generates contextualized insights that would otherwise be impossible to capture in purely quantitative or qualitative studies.

This approach differs from the positivist paradigm, which would favour purely quantitative measures of exposure (e.g., number of hours working with systems, frequency of security incidents). The proposed model suggests the need to combine both perspectives – objective indicators of technological exposure and subjective assessments of stress – leading to methodological triangulation. One of the key challenges is the operationalisation of cyber stress. The tools used so far, such as the technostress scale developed by Tarafdar et al. (2007, 2019), mainly measure the negative aspects of the phenomenon: information overload, technological uncertainty, and technology-related role conflict. The proposed model, on the other hand, assumes that cyberstress is ambivalent: in addition to its destructive effects (decreased productivity, anxiety, burnout), it can also have a mobilising effect, developing adaptive competences.

From a methodological point of view, this means that two-dimensional measurement tools need to be developed to measure both the level of stress and the adaptive potential of cyber stress. Psychological research on so-called eustress may serve as inspiration here (Simmons & Nelson, 2007). Extending existing scales with ‘constructive’ components would be a significant contribution to the literature and practice. The model clearly indicates the need for multilevel modelling. Cyber stress affects not only individuals, but also teams and entire organisations. This means that adequate research projects should cover:

1) the individual level (employee perception, digital competences, coping strategies),
2) team level (group cohesion, social support, distribution of responsibility for security),
3) organisational level (security culture, HR policy, risk management strategy).

Methodologically, this suggests the use of HLM (hierarchical linear modelling) or SEM-Multilevel models, which allow for the analysis of interactions between levels.

Taking safety culture into account as a moderator poses additional methodological challenges. Culture is a complex construct that is difficult to measure directly. The literature typically uses surveys based on employee perceptions (Reason, 1997), but triangulation – combining survey data, participant observation and analysis of organisational documents – is increasingly being suggested (Dekker, 2016). For the proposed model, it is important that safety culture is measured not only as the ‘presence of formal procedures,’ but also as the practised organisational climate – that is, the way in which employees actually interpret rules and respond to errors. The model also implies the need for mixed methods. Quantitative research allows us to test hypotheses about the relationship between cyber stress and resilience, while qualitative research allows us to understand the processes of sensemaking and narratives around cyber threats. Case studies in organisations that have experienced serious cybersecurity incidents may prove particularly valuable, as they allow us to analyse the dynamics of stress in real time. Another methodological implication is the need to conduct longitudinal studies. Cyberstress is processual in nature – its effects do not manifest themselves immediately, but evolve over time. In the short term, it can reduce work efficiency, but in the long term, with appropriate support, it can

lead to increased resilience. Designing studies in panel systems would allow this dynamic to be captured, avoiding simplistic conclusions based on cross-sectional studies.

TABLE 1: KEY METHODOLOGICAL IMPLICATIONS OF THE CYBER STRESS AND RESILIENCE MODEL

Model dimension	Role in the model	Indicators	Research metodhs
Digital environment pressure	Independent variable	Number of IT incidents, frequency of updates, self-assessment of technological burden	Analysis of system logs, surveys, observation
Cyberstres	Mediator	Technological stress scale (Tarafdar et al., 2019), extended by an adaptive component (eustress)	Psychometric questionnaires, qualitative interviews
Coping mechanisms	Mediating mechanism	Cognitive, emotional, behavioural strategies (according to Lazarus and Folkman, 1984)	Surveys, stress diaries, narrative analysis
Safety Culture	Moderator	Organisational climate indicators, level of trust, approach to errors	Surveys, case studies, document analysis
Organisational resilience	Outcome	Process recovery time, adaptability, team cohesion assessment	Longitudinal studies, comparative case analysis

Source: author's own elaboration

VI. PRACTICAL IMPLICATIONS OF THE MODEL FOR ORGANISATIONAL MANAGEMENT

The proposed model, which treats cyber stress as an intermediary variable between technological pressure and organisational resilience, generates a number of practical implications for contemporary management. Their significance extends beyond the narrow framework of IT security, as they combine the areas of human resource management, organisational psychology, strategy and crisis management. The first practical conclusion is the need to integrate IT security policy with human resource management policy. As research shows (Von Solms & Van Niekerk, 2013; Siponen et al., 2014), the traditional approach to cybersecurity focuses on technical procedures, ignoring the subjective experiences of employees. The introduction of cyber stress management programmes requires HR policies to include training in coping with digital stress, resilience mentoring and psychological support in the event of incidents. Such measures should be complemented by feedback systems that allow changes in stress levels among employees to be monitored. Another area is the role of organisational culture and leadership. Leaders who promote openness to discussing mistakes and build a climate of trust reduce the risk of cyber stress escalating. Research on psychological safety (Edmondson, 2019) shows that teams where employees are not afraid of the consequences of reporting problems are more resilient to external stressors. In practice, this means that managers should be trained in cyber-empathetic leadership, combining technological risk awareness with emotional support skills. The model also points to the need to implement training programmes that go beyond technical IT training. These should include:

1) mental resilience training (e.g. based on mindfulness, cognitive-behavioural coping strategies)(Podolak et all 2025) ,
2) crisis simulations (e.g. phishing attack, system failure),
3) team workshops to strengthen cooperation and trust.

This approach not only minimises the negative effects of cyber stress, but also transforms it into a potential source of growth in adaptive competences. The practical implementation of the proposed model also requires the development of cyber stress monitoring systems. These can take the form of regular surveys, anonymous problem reports, and even behavioural analyses based on system data (e.g., frequency of login errors, response time to system messages). Such solutions make it possible to design early warning systems that signal increasing employee workload and allow for rapid intervention.

VII. CONCLUSION

This article attempts to integrate two areas of research that have largely operated in parallel until now: cybersecurity management and organisational resilience psychology. The central element of the proposed model is cyber stress, treated not only as a negative effect of digitalisation, but as an intermediary variable that can have a destructive or mobilising effect depending on the organisational context. The conclusions drawn from the literature review and conceptual discussion are multidimensional. First, cybersecurity management should be viewed not only in technical terms, but also in psychosocial terms, which implies the need to integrate IT and HR policies. Secondly, security culture and supportive leadership become key moderators that determine whether cyber stress leads to burnout or growth. Thirdly, the development of training programmes and stress monitoring systems is an essential element in building resilience at the individual, team and organisational levels. From a scientific point of view, the proposed model opens up new fields of research, particularly in the operationalisation of the construct of cyber stress, longitudinal studies and multi-level analyses of resilience. From the point of view of managerial practice, it provides a framework for designing organisational policies that treat people not as the weakest link in the security system, but as active contributors to resilience. The key and most important message of the article is the need to change the perspective on cybersecurity – from a purely technological one to a holistic one that takes into account both technology and psychology. Only such an approach will allow organisations not only to survive in the era of digital threats, but also to thrive thanks to them, building resilient, aware and integrated security cultures.

VIII. REFERENCES

Alvesson, M., & Deetz, S. (2000). Doing critical management research. SAGE.

Alliger, G. M., Cerasoli, C. P., Tannenbaum, S. I., & Vessey, W. B. (2015). Team resilience: How teams flourish under pressure. Organizational Dynamics, 44(3), 176–184. https://doi.org/10.1016/j.orgdyn.2015.05.003

Antonovsky, A. (1987). Unraveling the mystery of health: How people manage stress and stay well. Jossey-Bass.

Antonsen, S. (2009). Safety culture: Theory, method and improvement. Ashgate.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. MIS Quarterly, 35(4), 831–858.

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Badawy, A., Dudau, A., & Sasse, M. A. (2021). Security fatigue and employee compliance. Computers & Security, 103, 102150. https://doi.org/10.1016/j.cose.2020.102150

Berger, P. L., & Luckmann, T. (1991). The social construction of reality. Penguin. (Original work published 1966)

Block, J., & Kremen, A. M. (1996). IQ and ego-resiliency: Conceptual and empirical connections and separateness. Journal of Personality and Social Psychology, 70(2), 349–361. https://doi.org/10.1037/0022-3514.70.2.349

Brod, C. (1984). Technostress: The human cost of the computer revolution. Addison-Wesley.

Burrell, G., & Morgan, G. (1979). Sociological paradigms and organisational analysis. Heinemann.

Clarke, S. (2013). Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. Journal of Occupational and Organizational Psychology, 86(1), 22–49. https://doi.org/10.1111/joop.12010

Connor, K. M., & Davidson, J. R. T. (2003). Development of a new resilience scale: The Connor–Davidson Resilience Scale (CD-RISC). Depression and Anxiety, 18(2), 76–82. https://doi.org/10.1002/da.10113

Cooper, C. L., Flint-Taylor, J., & Pearn, M. (2013). Building resilience for success: A resource for managers and organizations. Palgrave Macmillan.

Creswell, J. W., & Plano Clark, V. L. (2024). Designing and conducting mixed methods research (4th ed.). SAGE.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems, 31(2), 285–318. https://doi.org/10.1080/07421222.2014.995538

Day, A., Scott, N., & Kelloway, E. K. (2010). Information and communication technology: Implications for job stress and employee well-being. In P. L. Perrewé & D. C. Ganster (Eds.), New developments in theoretical and conceptual approaches to job stress (pp. 317–350). Emerald.

Dekker, S. (2016). Just culture: Restoring trust and accountability in your organization (3rd ed.). CRC Press.

Edmondson, A. C. (2019). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley.

ENISA. (2025). Cybersecurity and resilience report 2025. European Union Agency for Cybersecurity.

Eppler, M. J., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. The Information Society, 20(5), 325–344. https://doi.org/10.1080/01972240490507974

Farheen, F., Akhtar, M., & Khan, A. (2024). Cybersecurity resilience in emerging economies. Journal of Information Security, 18(2), 99–115.

Fletcher, D., & Sarkar, M. (2013). Psychological resilience: A review and critique of definitions, concepts, and theory. European Psychologist, 18(1), 12–23. https://doi.org/10.1027/1016-9040/a000124

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. Safety Science, 34(1–3), 215–257. https://doi.org/10.1016/S0925-7535(00)00014-X

Hollnagel, E. (2011). Resilience engineering in practice: A guidebook. Ashgate.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). Resilience engineering: Concepts and precepts. Ashgate.

INSAG. (1986). Summary report on the post-accident review meeting on the Chernobyl accident. International Atomic Energy Agency.

Introna, L. D. (2016). Algorithms, governance, and governmentality: On governing academic writing. Science, Technology, & Human Values, 41(1), 17–49. https://doi.org/10.1177/0162243915587360

Kobasa, S. C. (1979). Stressful life events, personality, and health: An inquiry into hardiness. Journal of Personality and Social Psychology, 37(1), 1–11. https://doi.org/10.1037/0022-3514.37.1.1

Korunka, C., & Vitouch, O. (2017). Job demands, resources and health: Work stress and burnout in digital environments. European Journal of Work and Organizational Psychology, 26(5), 694–706. https://doi.org/10.1080/1359432X.2017.1345880

Krasikova, D. V., Green, S. G., & LeBreton, J. M. (2013). Destructive leadership: A theoretical review, integration, and future research agenda. Journal of Management, 39(5), 1308–1338. https://doi.org/10.1177/0149206312471388

Kuhn, T. S. (2012). The structure of scientific revolutions (4th ed.). University of Chicago Press. (Original work published 1962)

Lazarus, R. S. (1999). Stress and emotion: A new synthesis. Springer.

Lazarus, R. S., & Folkman, S. (1984). Stress, appraisal, and coping. Springer.

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 21(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.07.002

LePine, J. A., Podsakoff, N. P., & LePine, M. A. (2016). A meta-analytic test of challenge and hindrance stress framework. Academy of Management Journal, 49(5), 764–775. https://doi.org/10.5465/amj.2006.23478217

Luthar, S. S., Cicchetti, D., & Becker, B. (2000). The construct of resilience: A critical evaluation and guidelines for future work. Child Development, 71(3), 543–562. https://doi.org/10.1111/1467-8624.00164

Maier, C., Laumer, S., Eckhardt, A., & Weitzel, T. (2019). Technostress and the hierarchical levels of personality: A two-wave study with multiple data samples. Information Systems Journal, 29(1), 122–152. https://doi.org/10.1111/isj.12197

Mazmanian, M., Orlikowski, W. J., & Yates, J. (2013). The autonomy paradox: The implications of mobile email devices for knowledge professionals. Organization Science, 24(5), 1337–1357. https://doi.org/10.1287/orsc.1120.0806

Meneghel, I., Salanova, M., & Martínez, I. M. (2016). Feeling good makes us stronger: How team resilience mediates the relationship between positive emotions and performance in teams. Journal of Happiness Studies, 17(1), 239–255. https://doi.org/10.1007/s10902-014-9592-6

Mizrak, F., Kaya, B., & Polat, Z. (2025). Organizational resilience in digital supply chains. International Journal of Logistics Management, 36(1), 77–95.

Mulki, J. P., Jaramillo, F., & Locander, W. B. (2006). Emotional exhaustion and organizational deviance: Can the right job and a leader's style make a difference? Journal of Business Research, 59(12), 1222–1230. https://doi.org/10.1016/j.jbusres.2006.09.001

Oladimeji, G. (2025). Cyber resilience in African SMEs. African Journal of Information Systems, 17(2), 45–61.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. Organization Science, 3(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

Orlikowski, W. J., & Scott, S. V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. Academy of Management Annals, 2(1), 433–474. https://doi.org/10.5465/19416520802211644

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Podolak, A., Zarotyńska, A., & Bieniara-Woźnicka, J. (2025). The impact of social pressure on men's mental health - analysis of social expectations from the perspective of clinical psychology. Scientific Journal of Bielsko-Biala School of Finance and Law, 29(1). https://doi.org/10.19192/wsfip.sj1.2025.9

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. Information Systems Research, 19(4), 417–433. https://doi.org/10.1287/isre.1070.0165

Reason, J. (1997). Managing the risks of organizational accidents. Ashgate.

Salanova, M., Llorens, S., & Cifre, E. (2013). The dark side of technologies: Technostress among users of information and communication technologies. International Journal of Psychology, 48(3), 422–436. https://doi.org/10.1080/00207594.2012.680460

Shu, Q., Tu, Q., & Wang, K. (2011). The impact of computer self-efficacy and technology dependence on computer-related stress. Computers in Human Behavior, 27(5), 2200–2206. https://doi.org/10.1016/j.chb.2011.06.020

Simmons, B. L., & Nelson, D. L. (2007). Eustress at work: Extending the holistic stress model. In D. L. Nelson & C. L. Cooper (Eds.), Positive organizational behavior (pp. 40–53). SAGE.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Skeoch, R. (2024). Team resilience in cybersecurity environments: Communication, trust and shared responsibility. Journal of Organizational Behavior, 45(2), 155–173.

Sonnentag, S., & Frese, M. (2013). Stress in organizations. In N. W. Schmitt & S. Highhouse (Eds.), Handbook of psychology: Industrial and organizational psychology (2nd ed., pp. 560–592). Wiley.

Stich, J. F., Tarafdar, M., Cooper, C. L., & Stacey, P. (2019). Workplace stress from actual and desired computer-mediated communication use: A multi-method study. Journal of Information Technology, 34(3), 196–213. https://doi.org/10.1177/0268396219856161

Tarafdar, M., Pullins, E. B., & Ragu-Nathan, T. S. (2015). Technostress: Negative effect on performance and possible mitigations. Information Systems Journal, 25(2), 103–132. https://doi.org/10.1111/isj.12042

Tugade, M. M., & Fredrickson, B. L. (2004). Resilient individuals use positive emotions to bounce back from negative emotional experiences. Journal of Personality and Social Psychology, 86(2), 320–333. https://doi.org/10.1037/0022-3514.86.2.320

Vaara, E., Sonenshein, S., & Boje, D. (2016). Narratives as sources of stability and change in organizations: Approaches to sensemaking through discursive and rhetorical strategies. Academy of Management Annals, 10(1), 495–560. https://doi.org/10.5465/19416520.2016.1161964

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Weber, M. (1978). Economy and society: An outline of interpretive sociology. University of California Press.

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). Wiley.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.