Scientific Studios on Social and Political Psychology

Journal homepage: https://sppstudios.com.ua/
***Scientific Studios on Social and Political Psychology*, 31(1), 6-15**

UDC 004.056.5:159.944:316.6
DOI: 10.61727/sssppj/1.2025.06

Digital transformation era: Impact of cybersecurity on workplace mental health

Oleh Starovoitenko*
PhD in Psychological Sciences, Senior Researcher
Institute of Social and Political Psychology of the National Academy of Educational Sciences of Ukraine
04070, 15 Andriivska Str., Kyiv, Ukraine
https://orcid.org/0009-0008-2886-1626

Abstract. The digital transformation of workplaces has profoundly impacted organisations around the world, introducing not only new efficiencies but also significant psychological and psychosocial risks for employees. While cybersecurity has traditionally has been considered as a technical concern, it increasingly poses mental health challenges for both IT professionals and general staff, particularly in the context of remote work and complex security protocols. This study aimed to identify and systematise common mental health issues related to cyber threats in organisational settings and to explore viable strategies for their prevention and mitigation. Combining a literature review with a targeted empirical survey, the research offered a view of the interaction between cybersecurity and employee well-being. Participants were non-cybersecurity professionals tasked with responding to cyber threats, providing unique insight into the mental strain associated with such responsibilities. Using inductive qualitative analysis and Likert-scale-based statistical evaluation, the study reveals that systemic, organisational-level interventions – such as clear cybersecurity policies, fairness in breach response, and appropriate training – are perceived as more effective in supporting mental health than individual psychological support services. These findings highlighted the urgent need to frame cybersecurity not only as a technical challenge but also as a core psychosocial issue. The research contributes to the growing field of cyberpsychology and offers practical recommendations for enhancing both digital and psychological resilience in modern organisations

Keywords: technostress; cyber threat; emotional stress; burnout; information overload

INTRODUCTION

The digital transformation of the workplaces has fundamentally reshaped the modern world. New technologies, practices, and paradigms for organisational functioning are being introduced at unprecedented and alarming speed. On the one hand, cloud computing, artificial intelligence, big data analytics, and remote work infrastructures have created opportunities for increased efficiency, innovation, and global connectivity. On the other hand, these technological advancements also introduce significant psychological and psychosocial risks for employees, particularly when they are implemented without appropriate consideration of human factors and cybersecurity threat landscape. The COVID-19 pandemic also made a great contribution into the widening gap between growing demands to the employees to cope with cyberthreat induced stress and their ability to do so. For instance, M. Vasilenko *et al.* (2020) analysed the cybersecurity and privacy concerns arising from the shift to remote work during the COVID-19 pandemic and identified

Article's History: Received: 04.03.2025 Revised: 17.05.2025 Accepted: 23.06.2025

Suggested Citation:
Starovoitenko, O. (2025). Digital transformation era: Impact of cybersecurity on workplace mental health. *Scientific Studios on Social and Political Psychology*, 31(1), 6-15. doi: 10.61727/sssppj/1.2025.06.

*Corresponding author

new risks, including heightened stress, and the adoption of surveillance technologies, which can compromise employee privacy and well-being.

As organisations invest heavily in digital infrastructures, they become increasingly vulnerable to cyber threats such as data breaches, ransomware attacks, phishing schemes, and many other threats that in addition to technical and financial risks also contribute to heightened psychological strain on employees tasked with safeguarding digital assets. Frontline cybersecurity professionals often experienced chronic stress, burnout, and "alert fatigue" due to the high-stakes and fast-paced nature of their work environments; however, non-technical employees also suffered from anxiety, confusion, or technostress when required to comply with complex security protocols or adapt to rapidly changing digital tools (Atrian & Ghobbeh, 2023). With non-professionals being affected with cybersecurity threats, it has now become obvious, that cybersecurity has already transitioned from a technical issue to a core organisational concern bringing new psychosocial risks, as employees across all sectors are exposed to cyberthreats such as phishing, data breaches, ransomware, and cyber harassment. Furthermore, digital transformation, stimulated by high pace of progress, COVID-19 pandemic and other global factors, such as current geopolitical situation are adding more and more weight to the role of cybersecurity domain in defining aggregate security and well-being of the humans. This makes the problem of interrelations between the manner in which cybersecurity is handled in organisations and mental health of the employees more and more essential.

Study by S. Arora & J.D. Hastings (2024) surveyed 50 cybersecurity professionals, revealing that 44% experienced severe work-related stress and burnout. The demanding nature of cybersecurity roles, coupled with unrealistic expectations and unsupportive organisational cultures, were identified as primary stressors. Notably, 66% of respondents perceived cybersecurity jobs as more stressful than other IT positions, with 84% facing additional challenges due to the pandemic and recent high-profile breaches. Based on the respondents' feedback, the researchers recommended fostering supportive work environments and implementing mindfulness programs to address these issues. One of the traditional ways for creation of supportive environments is the integration of cybersecurity awareness with organisational psychology strategies – for example, embedding emotional resilience and digital mindfulness in cybersecurity training. Moreover, mental health support services tailored to employees affected by data breaches or cyberbullying are emerging as best practices in high-risk sectors such as finance, health, and education (Ivanova *et al.*, 2024). However, there is also evidence, that active exposure to cybersecurity training and simulated threats (e.g., phishing simulations) can induce a sense of hyper-vigilance and lead to "security fatigue", a condition where individuals feel overwhelmed and disengaged from secure behaviour.

A study by S. Khadzhyradieva *et al.* (2024) analysed cyber-psychological protection programs within Ukraine's education system. The research highlighted the importance of these programs in enhancing awareness among students, educators, and administrative staff regarding potential cyber threats. The study, among other things, recommended exploring external resources, fostering collaboration, and establishing standardised measures to ensure effective cyber-psychological protection in education. K. Ihnatenko & S. Sadzaglishvili (2023) examined how Ukrainian organisations adapt to digital transformation during the war, emphasising the psychological toll on employees. The research found that the shift to remote work, coupled with constant cyber threats and physical dangers, led to increased stress and burnout. One of the key responses to the threat became organisations reintroducing psychological support services, including online counselling, to help employees cope with the heightened pressures. Recent studies emphasise the psychological burden of cybersecurity threats on employees. Cyberattack exposure, or even the perceived risk of being hacked, has been associated with increased levels of stress, anxiety, and reduced job satisfaction (Hadlington, 2017).

Based on the study of existing research, the aim of the article was to identify and systematise typical mental health problems observed among employees of various organisations in connection with cyberthreats and cybersecurity tasks, as well as to identify and systematise different solutions to prevent these issues. By conducting a survey of employees from various Ukrainian companies and organisations, aimed to validate the results of the literature review within the context of society. Analysing data on the relationship between cybersecurity and mental health in organisations would improve the systematisation of knowledge, highlight existing gaps, and outline future research areas in this field. Addressing this task will undoubtedly helped resolve various mental health problems associated with cybersecurity issues and suggest ways to improve cyber defence systems in modern organisations.

MATERIALS AND METHODS

The proposed study combines theoretical and applied parts aiming to identify typical mental health problems associated with cybersecurity issues, along with typical solutions. To achieve the declared research goal, a review of relevant and significant studies on mental health issues related to cybersecurity was conducted. The list of analysed studies included those published over the last 15 years. This allowed to identify key issues and potential solutions. The study was focused on publications that examined both the issues and potential solutions. Only studies published in English were selected. All studies underwent inductive

qualitative analysis to identify sets of typical mental health problems related to cybersecurity and possible coping solutions.

Based on these sets, there was conducted a survey of government employees and employees of commercial companies regarding their experiences with cyber threats and the related mental health challenges. The study participants included 20 employees from various Ukrainian public organisations and private companies who, according to their job responsibilities, are required to respond to cyber threats and make appropriate decisions, although they are not cybersecurity professionals. In the course of the study, compliance with ethical standards was ensured in accordance with American Sociological Association's Code of Ethic (1997). The study employed inductive qualitative analysis and the psychometric Likert scale.

RESULTS AND DISCUSSION

The way an organisation handles cyber incidents plays a crucial role in shaping employees' psychological responses. A lack of transparent communication, poor incident response management, and blaming culture can aggravate emotional distress, decrease organisational trust, and increase attrition risk. Conversely, psychologically safe environments foster resilience and quicker recovery after cybersecurity incidents. The issue of mental health and cybersecurity interplay, there exists a significant body of research executed within certain theories and frameworks originating from the organisational psychology domain. For instance, the E. Demerouti *et al.* (2001) model, has become a central framework in occupational health psychology to explain how job demands lead to burnout and how job resources support engagement and well-being. Scholars increasingly more often have begun integrating cybersecurity-related stressors into this model, examining how cyberthreats – such as phishing, ransomware, surveillance, and digital overload – function as novel job demands that deplete employee resources and contribute to negative mental health outcomes.

Cyberthreats also lead to a state of hypervigilance, where employees experience a perceived constant risk of attack, which consumes emotional and attentional resources. According to N.S. Safa & R. Von Solms (2016), this state can activate a threat appraisal response, increasing the risk of psychological strain, especially when organisational support is lacking. Several studies emphasised the absence or insufficiency of job resources – such as supportive leadership, clear communication, digital autonomy, and psychological safety – in the face of cyberthreats. This imbalance fosters resource depletion, as outlined in the Job Demands-Resources (JD-R) model, and leads to burnout, disengagement, and role ambiguity (Robert & Karasek, 1979). On the positive side, research within the JD-R framework also highlighted that psychosocial and organisational resources – such as informational transparency, cybersecurity self-efficacy, participative decision-making, and mindfulness training – can buffer the effects of cyber demands.

The Job Demand-Control (JDC) model by R. Karasek (1979) suggests that psychological strain arises when job demands are high and decision latitude (control) is low. In this framework, cybersecurity threats act as modern, high-stakes demands that tax cognitive and emotional resources, especially in digitally intensive work environments. When employees have little control over how to manage these cyber-demands or lack adequate support, the risk of mental health deterioration (e.g., anxiety, depression, burnout) increases. The JDC model predicted strain when employees face high demands with low control – a frequent scenario in cybersecurity compliance. Employees often reported: no influence over security policies; limited autonomy in handling risky situations; punitive consequences for small security lapses, and the research showed that this combination leads to occupational strain, increased anxiety, and in some cases, withdrawal behaviours (D'Arcy *et al.*, 2014).

R.W. Rogers (1975), posits that individuals adopt protective behaviours when confronted with perceived threats, especially if they believed in the severity of the threat, their vulnerability, the efficacy of the recommended protective behaviour, and their self-efficacy to carry it out. Fear is seen as a motivating emotion, prompting protective behaviour if cognitive appraisals align positively. In the context of organisations, cybersecurity threats – such as phishing, ransomware, data breaches, and insider threats – have become salient stressors. PMT provided a useful framework to understand how cyberthreat-induced fear impacts employees' mental states and behavioural responses. A large body of research has applied PMT to evaluate the effectiveness of fear-based cybersecurity messages. While fear appeals can be an effective motivator, PMT research warns that over-reliance on threat-based communication may backfire. Prolonged exposure to cyber fear stimuli without proper support mechanisms may leaded to techno-anxiety, job dissatisfaction, and mental fatigue. Cybersecurity communication strategies must balance threat salience with empowerment, aligning with employee mental health needs.

Social Exchange Theory (SET) (Blau, 1964) suggested that workplace relationships are governed by reciprocal exchanges between employees and their organisations. When employees perceive fair and supportive treatment, they are more likely to demonstrated loyalty, commitment, and well-being. Conversely, when the exchange is perceived as imbalanced, coercive, or unsafe, employees may experience emotional exhaustion, withdrawal, and mental distress. In the context of cybersecurity, organisations increasingly demand employees' vigilance, compliance, and adaptability – often without

offering corresponding support, autonomy, or emotional compensation. This perceived breach of the psychological contract can lead to stress-related outcomes. When employees perceive these demands as excessive or unjustified, especially in the absence of adequate training or appreciation, the perceived reciprocity diminishes. This perceived imbalance can foster emotional exhaustion and diminished well-being. SET-related studies showed that when employees feel exploited or under-supported, especially in high-risk environments like cybersecurity, they may experience: anxiety and helplessness, due to unclear expectations or blame for breaches; job dissatisfaction, due to the coercive or punitive culture of security enforcement; withdrawal behaviour, including burnout and reduced organisational citizenship behaviour. Studies by C. Posey *et al.* (2011) and N. Safa & R. Von Solms (2016) illustrated how trust erosion in cybersecurity policies leads to resistance, disengagement, and stress symptoms.

Technostress theory refers to the stress experienced by individuals due to their inability to cope with information and communication technologies (ICTs) in a healthy manner. First introduced by C. Brod (1984), technostress definition has evolved to include dimensions such as techno-overload, techno-invasion, techno-complexity, techno-insecurity, and techno-uncertainty. There is a growing body of research showing that emergence of cyberthreats – including phishing, data breaches, ransomware, and insider threats – has intensified technostress in organisations. Employees are increasingly required to comply with cybersecurity protocols, remain vigilant, and adapt to rapidly evolving digital environments, which may result in both negative psychological strain and positive adaptation outcomes. Technostress was studied, for instance, by A. Atrian & S. Ghobbeh (2023) as a stress induced by rapid technological changes in the workplace. Their research highlighted that technostress adversely affects job performance, leading to decreased productivity and increased turnover intentions. However, it is worth mentioning, that despite its negative framing, technostress also has positive facets, such as techno-eustress, which refers to stress that leads to growth, adaptation, and improved performance (Tarafdar *et al.*, 2019). Employees may develop cyber-resilience, improve technical competence, and gain a stronger sense of digital self-efficacy in response to cyberthreats when appropriate support and training are provided.

Organisational Justice Theory (Greenberg, 1987) refers to employees' perceptions of fairness in workplace processes, distributions, and interpersonal interactions. The theory comprises three main components: distributive justice – fairness in resource allocation (e.g., who bears cybersecurity responsibilities); procedural justice – fairness in decision-making processes (e.g., how cybersecurity policies are developed and enforced); interactional justice – fairness in interpersonal treatment and communication (e.g., respectful and clear cybersecurity communication). When justice is perceived as lacking – particularly during the implementation of cyber-related procedures – psychological strain and mental health consequences can arise. Several studies have demonstrated that perceptions of low fairness in security demands result in: increased emotional exhaustion; higher anxiety levels in high-surveillance digital environments; feelings of helplessness and role ambiguity, especially among non-IT staff (Johnston *et al.*, 2016). Employees who perceive greater justice in security policies – through transparent communication, employee participation, and supportive culture – report lower psychological strain and higher engagement. Summing up the recommendations developed within the organisational justice theory, the following steps will be recommended to mitigate mental health risks linked to cyberthreat-related practices: involving employees in cybersecurity policy development (Herath & Rao, 2009); communicating decisions with empathy and clarity; ensuring fairness in responsibility assignment and response to breaches (Cheng *et al.*, 2013). Inductive qualitative analysis was applied to all of the aforementioned studies with the aim of developing sets of typical mental health problems related to cyberthreats and possible solutions to them. The results are presented in Table 1.

Table 1. Typical mental health issues connected with cyberthreats and typical solutions to prevent health issues connected with cyberthreats

higher anxiety	*constructive feedback on cyberthreats and cyber incidents*
psychological strain	
mental stress symptoms	*moderate level of cybersecurity demands*
increased emotional exhaustion	*ensuring fairness in responsibility assignment and response to breaches*
burnout	
increased cognitive load	*involving employees in cybersecurity policy development and relevant decision-making*
vigilance fatigue	
fear of making security mistakes or cyber anxiety	*clear cybersecurity policies and protocols*
job dissatisfaction	*empathetic leadership: communicating decisions with empathy and clarity*
decreased productivity	

Table 1, Continued

feeling of role ambiguity or role conflict	*provision of appropriate support and training*
defensive avoidance	
withdrawal behaviour or disengagement	*psychological support services in organisations*
feelings of helplessness	

Source: compiled by the author

Next, there was conducted a survey of 20 employees from various Ukrainian public organisations and private companies whose job responsibilities involve responding to cyberthreats and making corresponding decisions. Each participant was asked to evaluate each mental health problem related to cybersecurity using a rating scale similar to a 5-point Likert scale, ranging from 1 to 5: never encountered, occasionally encountered, periodically encountered, frequently encountered, constantly encountered. They were also asked to rate each of the proposed solutions to mental health problems related to cybersecurity using a similar 5-point Likert-type scale, ranging from 1 to 5: not efficient, rather not efficient, possibly efficient, rather efficient, definitely efficient. The scores were then summed, and the average values were calculated and presented in Figures 1 and 2. The problems and solutions were ranked based on their average scores, which were interpreted as indicators of the probability of a particular issue and the efficiency of a particular solution as perceived by the participants of the survey.

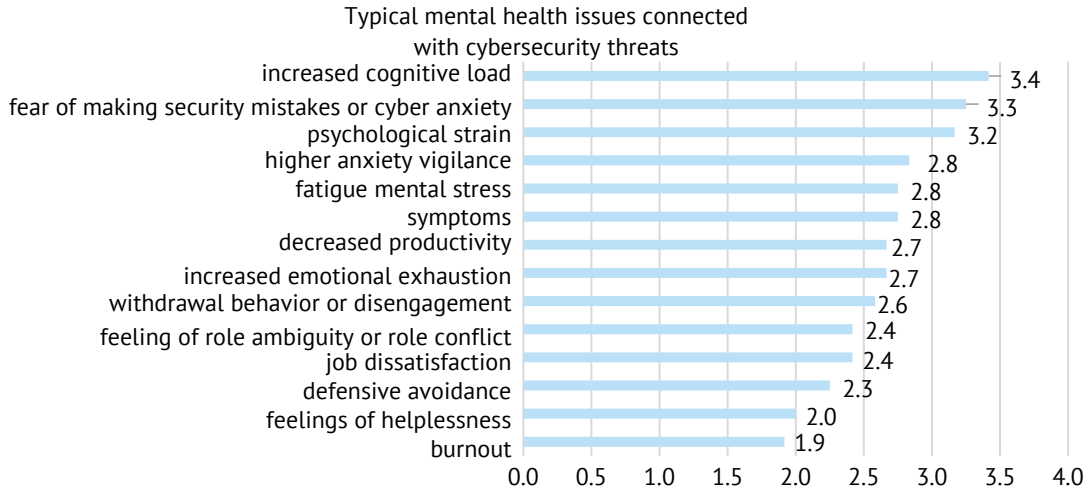

Figure 1. Probability of typical mental health issues connected with cyberthreats based on the results of the empirical study

Source: compiled by the author

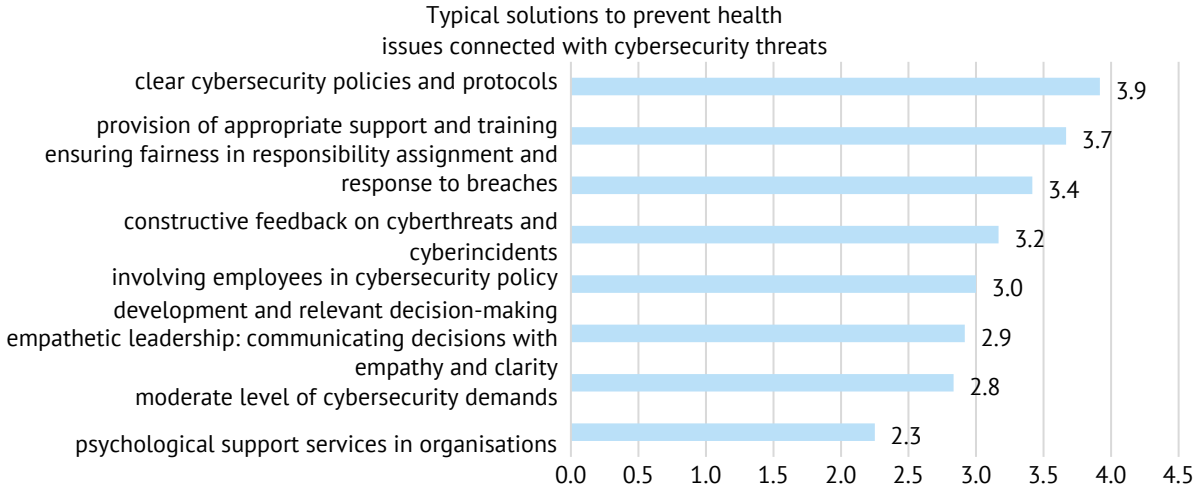

Figure 2. Expected efficiency of typical solutions to prevent health issues connected with cybersecurity threats based on the results of the empirical study

Source: compiled by the author

Overall, the obtained survey measurement results were assessed as consistent with the findings of the reviewed research literature and as interpretable in a clear and straightforward manner. Most typical issues and possible solutions received sufficiently high average scores, which supports the interpretation of these results as evidence of the content validity of the theoretical part of study. The scores indicate how frequently employees in cybersecurity-sensitive roles encounter specific mental health challenges. These results reveal a clear gradient in perceived impact, ranging from frequently encountered experiences such as increased cognitive load (mean = 3.4) to lower-intensity issues like burnout (mean = 1.9). High-scoring issues, or those frequently experienced, included increased cognitive load (3.4); fear of making mistakes/cyber anxiety (3.3); psychological strain (3.2). The high score on cognitive load reflects the mental intensity required to maintain security vigilance and decision-making under pressure. Moderate-scoring issues (periodic issues) included mental stress symptoms, vigilance fatigue, and anxiety (2.8); emotional exhaustion and reduced productivity (2.7); disengagement/withdrawal (2.6); role ambiguity/conflict (2.4); job dissatisfaction (2.4) clearly demonstrate that continuous alertness demands in cybersecurity-connected roles are taking a psychological toll. The relatively low scores of defensive avoidances (2.3); feelings of helplessness (2.0) and burnout (1.9) suggest that complete emotional exhaustion and disengagement are not typical for the participants of the survey, which lets presume that mental health issues connected with cyber threats are not overwhelming for the participants. On the other hand, there is a clear trend toward cognitive and emotional overload, with high scores in anxiety, cognitive strain, and psychological stress.

Based on the survey results provided, also conducted an analysis regarding organisational preferences for addressing mental health issues related to cyberthreats. The data represents mean scores of perceived efficiencies (assumed to be on a Likert scale, where a higher score reflects a greater perceived efficiency). Survey indicated that among solutions to potential mental health issues connected with cyberthreats in organisations the top-rated are: the availability of clear cybersecurity policies and protocols (3.9); provision of support and training (3.7); fairness in breach response (3.4). All belong to formal, organisational group of solutions, aimed at systemic, organisation-wide approach. The moderately high scores for fair responsibility assignment (3.4) and constructive feedback (3.2) indicate a preference for transparent, fair, and practice-oriented approaches to managing incidents, which is consistent with high scores of organisational groups of solutions. These middle-range scores of employee involvement (3.0) and empathetic leadership (2.9) imply that while empathy and inclusion are valued, they are seen as supplementary, not central. Survey participants might appreciate these features but may not view them as strong mitigators of mental health stress arising from cyberthreats. A surprisingly low score for psychological support services (2.3) might suggest either stigma, still surrounding psychological help organisational cultures, or preference for being focused on coping with the root problem, that is with the cyber threats, instead of trying to remediate their impact on mental health.

Recent research shows that cybersecurity incidents and related organisational vigilance measures (e.g., frequent password changes, phishing simulations, digital surveillance, zero-trust policies) are increasingly perceived by employees as cognitive and emotional job demands. These demands increase workload, decision fatigue, and techno-stress, all of which are strongly associated with emotional exhaustion – a core component of burnout (Molino *et al.*, 2020).

For instance, when employees receive clear protocols and emotional support after a cyber incident, the risk of burnout significantly decreases (Sonnentag *et al.*, 2021). Leadership also plays a crucial role. Transformational leadership styles have been associated with higher engagement and lower stress levels in cyber-vulnerable sectors like finance and healthcare (Ayyagari *et al.*, 2011). Digital transformation has introduced new occupational stressors stemming from increased exposure to cyberthreats, such as: constant vigilance for phishing or malware; mandatory compliance with stringent cybersecurity protocols; regular password changes, two-factor authentication, and security audits; fear of human error leading to security breaches. Studies showed that these activities represented a cognitive and emotional burden, especially when perceived as mandatory and inflexible (Hadlington, 2017). It is worth mentioning that digital surveillance and monitoring, common in cybersecurity regimes, can further reduce perceived control and increase psychological tension. Empirical research (Moore *et al.*, 2018) shows that cybersecurity systems often operate with limited transparency, contributing to a culture of fear and eroding trust in management. Studies by P. Ifinedo (2012) and A. Johnston *et al.* (2016) found that moderate levels of fear, when accompanied by high efficacy messages, are effective in promoting secure behaviour. However, if fear appeals are too intense or frequent, they may induce learned helplessness, anxiety, or disengagement, especially when organisational support is perceived as low.

Research showed that frequent exposure to cyberthreat-related communications – such as simulated attacks or alerts – can heighten perceived vulnerability and trigger chronic fear, which is associated with emotional exhaustion, anxiety, and cognitive overload. S.R. Boss *et al.* (2015) demonstrated that employees' protective behaviour is significantly influenced by both perceived threat severity and psychological costs, such as fear of blame or punishment after a breach.

The mental health impact of fear-based cybersecurity interventions is mediated by self-efficacy and organisational safety culture. H.-S. Rhee *et al.* (2009) founded those individuals with high cybersecurity self-efficacy are more likely to react constructively to fear appeals. Conversely, when self-efficacy is low, fear leads to defensive avoidance and mental strain, especially in high-stakes environments like healthcare and finance. Supportive environments that offer clear protocols, psychological safety, and constructive feedback reduce the risk of fear-induced burnout or stress (Söllner *et al.*, 2016). However, strategic interventions, such as training programs and supportive leadership, can mitigate these negative effects.

Cybersecurity practices, such as mandatory multi-factor authentication, complex password requirements, security awareness training, and email vigilance, can contribute to techno-overload and techno-complexity. Studies J.R.C. Nurse *et al.* (2021) showed that such demands increase cognitive load, role conflict, and emotional exhaustion – predictors of burnout and reduced job satisfaction. However, strategic interventions, such as training programs and supportive leadership, can mitigate these negative effects. Cybersecurity practices, such as mandatory multi-factor authentication, complex password requirements, security awareness training, and email vigilance, can contribute to techno-overload and techno-complexity. Studies (Ragu-Nathan *et al.*, 2008) showed that such demands increase cognitive load, role conflict, and emotional exhaustion – predictors of burnout and reduced job satisfaction.

J. D'Arcy *et al.* (2014) highlighted how increased cyber risk awareness and fear of making security mistakes may cause techno-insecurity, especially in sectors with high compliance pressure such as healthcare, finance, and education. Prolonged exposure to cyber risk scenarios may contribute to cyber anxiety, vigilance fatigue, insomnia, and techno-phobia. These effects are especially pronounced among older employees or those with lower digital literacy (Salanova *et al.*, 2013). Recent studies during the post-COVID remote work transition (Spagnoli *et al.*, 2020) showed that the intensification of digital surveillance and cybersecurity monitoring has led to perceptions of techno-invasion, affecting work-life balance and psychological well-being. A supportive organisational climate can moderate the negative mental health outcomes of technostress. Clear cybersecurity policies, empathetic leadership, employee involvement in decision-making, and flexible response protocols are associated with reduced anxiety, higher compliance, and lower technostress levels. Conversely, ambiguity in cybersecurity communication, frequent software updates, or alarmist messaging can increase techno-uncertainty and foster a culture of fear and disengagement (Maier *et al.*, 2015). Employees exposed to moderate cybersecurity demands, accompanied by clear communication and autonomy, reported higher engagement and adaptive coping mechanisms, such as proactive learning and collaboration with IT departments. The data obtained in this study showed that the results did not fully align with the findings of other researchers. This partial discrepancy indicated the complexity of the issue under investigation and pointed to the necessity of conducting more in-depth research to explore the underlying factors, refine existing approaches, and expand the current understanding of the subject matter.

CONCLUSIONS

In general, based on the survey results it was assumed employees prioritise clarity, fairness, and competency-building over reactive or emotional support. They seek predictability and preparedness in their work environment as buffers against cyber-related psychological stress.

From a psychological perspective, employees favour pragmatic, system-wide strategies that increase their sense of control, predictability, and fairness in responding to cyberthreats. The data demonstrated that formal organisational solutions – such as clear cybersecurity protocols, targeted training, and fair distribution of responsibility – were evaluated as more effective than psychological counselling or emotional support services. This tendency might reflect an embedded organisational culture that values direct competence-building over remedial interventions.

While psychological strain, cognitive overload, and cyber-related anxiety emerged as frequently experienced issues, severe outcomes such as burnout or complete disengagement received notably lower ratings. This indicated that although cybersecurity-related stress was present, it had not yet escalated into chronic dysfunction for most respondents. Nevertheless, the consistent presence of emotional tension underscored the need for more resilient and supportive frameworks. Survey participants also associated higher perceived effectiveness with fairness in breach responses, constructive feedback, and access to training. Conversely, emotional or psychological support services received lower efficiency scores, which may indicate residual stigma or a preference for proactive, embedded resilience strategies.

In summary, the study confirmed the importance of aligning cybersecurity management with mental health safeguarding through transparent communication, fair governance, and participative approaches. Organisational resilience in the cybersecurity domain should integrate both technical and psychosocial resources to address the multifaceted nature of cyber-related mental strain. Future research might include collecting expert opinions on mental health issues connected with cyberthreats in organisations and possible solutions to them, inclusion of more

participants into survey, and studying correlations between identified issues and solutions.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] American Sociological Association's Code of Ethics. (1997). Retrieved from https://www.asanet.org/about/ethics/.
[2] Arora, S., & Hastings, J.D. (2024). A survey-based quantitative analysis of stress factors and their impacts among cybersecurity professionals. In *Proceedings of the 58th annual Hawaii international conference on system sciences* (pp. 6161-6160). Waikoloa Village: Hilton. doi: 10.48550/arXiv.2409.12047.
[3] Atrian, A., & Ghobbeh, S. (2023). Technostress and job performance: Understanding the negative impacts and strategic responses in the workplace. *ArXiv.*. doi: 10.48550/arXiv.2311.07072.
[4] Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly*, 35(4), 831-858. doi: 10.2307/41409963.
[5] Blau, P.M. (1964). Justice in social exchange. *Sociological Inquiry*, 34(2), 193-206. doi: 10.1111/j.1475-682X.1964.tb00583.x.
[6] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864. doi: 10.25300/MISQ/2015/39.4.5.
[7] Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Boston: Addison-Wesley.
[8] Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459. doi: 10.1016/j.cose.2013.09.009.
[9] 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. doi: 10.2753/MIS0742-1222310210.
[10] Demerouti, E., Bakker, A.B., Nachreiner, F., & Schaufeli, W.B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology*, 86(3), 499-512. doi: 10.1037/0021-9010.86.3.499.
[11] Greenberg, J. (1987). A taxonomy of organisational justice theories. *Academy of Management Review*, 12(1), 9-22. doi: 10.5465/amr.1987.4306437.
[12] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), article number e00346. doi: 10.1016/j.heliyon.2017.e00346.
[13] Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125. doi: 10.1057/ejis.2009.6.
[14] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. doi: 10.1016/j.cose.2011.10.007.
[15] Ihnatenko, K., & Sadzaglishvili, S. (2023). The digitalization of social services in response to the war in Ukraine. *Social Work and Education*, 10(3), 282-291. doi: 10.25128/2520-6230.23.3.2.
[16] Ivanova, O.S., Kit, N., & Storozhyk, M. (2024). Philosophy of education in the context of digital transformation of public life. *Humanities Studios: Pedagogy, Psychology, Philosophy*, 12(1), 141-148. doi: 10.31548/hspedagog15(1).2024.141-148.
[17] Johnston, A.C., Söllner, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231-251. doi: 10.1057/ejis.2015.15.
[18] Karasek, R.Jr. (1979). Job demands, job decision latitude, and mental strain: Implications for job redesign. *Administrative Science Quarterly*, 24(2), 285-308. doi: 10.2307/2392498.
[19] Khadzhyradieva, S., Todorova, M., Staikutsa, S., Tsybukh, L., & Lukiianchuk, A. (2024). Analysis of cyber-psychological protection programs in the education system: Role, limitations, and prospects. *Salud, Ciencia y Tecnología – Serie de Conferencias*, 3, article number 648. doi: 10.56294/sctconf2024.648.
[20] Molino, M., Ingusci, E., Signore, F., Manuti, A., Giancaspro, M.L., Russo, V., & Cortese, C.G. (2020). Wellbeing costs of technology use during Covid-19: The role of psychological detachment, technostress, and burnout. *Sustainability*, 12(15), article number 5911. doi: 10.3390/su12155911.
[21] Moore, P.V., Upchurch, M., & Whittaker, X. (2018). *Humans and machines at work: Monitoring, surveillance and automation in contemporary capitalism*. Cham: Palgrave Macmillan. doi: 10.1007/978-3-319-58232-0.

[22] Nurse, J.R.C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre- and post-COVID-19: An analysis of new threats and risks to security and privacy. In *HCI international 2021 – posters. Communications in computer and information science* (pp. 583-590). Cham: Springer. doi: 10.1007/978-3-030-78645-8_74.

[23] Posey, C., Bennett, R.J., & Roberts, T.L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6-7), 486-497. doi: 10.1016/j.cose.2011.05.002.

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

[25] Rhee, H.-S., Kim, C., & Ryu, Y.U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816-826. doi: 10.1016/j.cose.2009.05.008.

[26] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114. doi: 10.1080/00223980.1975.9915803.

[27] Safa, N.S., & Von Solms, R. (2016). An information security knowledge sharing model in organisations. *Computers in Human Behavior*, 57, 442-451. doi: 10.1016/j.chb.2015.12.037.

[28] 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. doi: 10.1080/00207594.2012.680460.

[29] Söllner, M., Hoffmann, A., & Leimeister, J.M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, 25(3), 274-287. doi: 10.1057/ejis.2015.17.

[30] Sonnentag, S., Dormann, C., & Demerouti, E. (2010). *Not all days are created equal: The role of daily job demands and resources for employee well-being*. Retrieved from https://www.researchgate.net/publication/254880606_Not_all_days_are_created_equal_The_concept_of_state_work_engagement.

[31] Spagnoli, P., Molino, M., Molinaro, D., Giancaspro, M.L., Manuti, A., & Russo, V. (2020). Workaholism and technostress during the COVID-19 emergency: The crucial role of the leaders on remote working. *Frontiers in Psychology*, 11, article number 620310. doi: 10.3389/fpsyg.2020.620310.

[32] Tarafdar, M., Cooper, C.L., & Stich, J.F. (2019). The technostress trifecta – techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal*, 29(1), 6-42. doi: 10.1111/isj.12169.

[33] Vasilenko, M., Novikov, V., Rachuk, V., & Slatvinska, V. (2020). Cybersecurity in the manifestations of risks during the pandemic period: Condition and genesis. *Bulletin of Cherkasy State Technological University*, 25(3), 30-39. doi: 10.24025/2306-4412.3.2020.214774.

Ера цифрової трансформації: вплив кібербезпеки на ментальне здоров'я в організаціях

Олег Старовойтенко

Кандидат психологічних наук, старший науковий співробітник
Інститут соціальної та політичної психології Національної академії педагогічних наук України
04070, вул. Андріївська, 15, м. Київ, Україна
https://orcid.org/0009-0008-2886-1626

Анотація. Цифрова трансформація робочих місць глибоко вплинула на організації по всьому світу, запровадивши не лише нові можливості для підвищення ефективності, але й значні психологічні та психосоціальні ризики для працівників. Хоча кібербезпека традиційно розглядається як технічна проблема, вона все частіше створює виклики для психічного здоров'я як для ІТ-фахівців, так і для загального персоналу, особливо в контексті віддаленої роботи та складних протоколів безпеки. Це дослідження мало на меті визначити та систематизувати загальні проблеми психічного здоров'я, пов'язані з кіберзагрозами в організаційному середовищі, а також дослідити життєздатні стратегії для їх запобігання та пом'якшення. Поєднуючи огляд літератури з цільовим емпіричним опитуванням, було запропоновано погляд на взаємозв'язок між кібербезпекою та благополуччям працівників. Учасники дослідження, які не були фахівцями з кібербезпеки, мали завдання реагувати на кіберзагрози, що дозволило їм отримати унікальне уявлення про психологічне навантаження, пов'язане з такими обов'язками. Використовуючи індуктивний якісний аналіз і статистичну оцінку за шкалою Лайкерта, дослідження показало, що системні заходи на організаційному рівні – такі як чітка політика кібербезпеки, справедливе реагування на порушення і відповідне навчання – сприймаються як більш ефективні для підтримки психічного здоров'я, ніж індивідуальні служби психологічної підтримки. Ці висновки підкреслили нагальну потребу розглядати кібербезпеку не лише як технічний виклик, а й як ключову психосоціальну проблему. Дослідження є внеском у розвиток кіберпсихології та пропонує практичні рекомендації щодо підвищення як цифрової, так і психологічної стійкості в сучасних організаціях

Ключові слова: технострес; кіберзагроза; емоційний стрес; вигорання; інформаційне навантаження