EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

COGNITIVE LOAD AND THE "URGENCY TRAP" WITH HYBRID WORK ENVIRONMENTS

SERGEI A. ZHUIKOV
EC-COUNCIL UNIVERSITY

PSY 360: Introduction to Social Psychology
Dr. Kathryn A. Henderson
February 27, 2026

Cognitive Load and the "Urgency Trap" with Hybrid Work Environments

Introduction

As a result of hybrid work arrangements, there has been a complete change in the relationship employees have with information systems and organizational assets. This change is more than just physical location changes; it has created a mental condition, Workplace Telepressure After Hours (WTA), in which an employee constantly thinks about how they must respond to work-related communications when they are not working (He et al., 2024). This constant mental engagement reduces the cognitive resources necessary for threat recognition and for behaving securely, creating an "urgency trap" in which time pressures and cognitive overload systematically combine to create vulnerabilities for threat actors to exploit (Cambier & Vlerick, 2022). With technology playing a bigger role in workplaces than ever before, there has been an increase in blending work and personal lives, as well as in where people work from. As research shows, employees are experiencing remarkably high levels of work overload, as seen in the mismatch between what they need to do (job demand) and the resources (personal resources) they must use to meet those demands (Kim et al., 2024). This overload influences cybersecurity behavior by decreasing an individual's ability to recognize potential threats and comply with security protocols, as well as limiting the use of proactive security behaviors (Kim et al., 2024). The intersection of cognitive load theory, telepressure phenomenon, and cybersecurity behaviors demonstrates that, no matter how advanced the technical controls are, they cannot be effective when users are under cognitive overload (Kritika, 2025).

Investigating cognitive load and urgency trap in hybrid working teams is an important research topic not only from an academic viewpoint, but also for providing practical security for organizations. Cybersecurity threat actors are increasingly using social engineering tactics to exploit psychological biases that rely on time constraints. Therefore, researchers must understand the cognitive and psychological elements that put employees at risk (Aschwanden et al., 2024). The recent COVID-19 pandemic has accelerated the integration of hybrid work, but it has also magnified these issues, making research on this topic an extremely relevant area for today's organizations (Cambier & Vlerick, 2022).

This research will fill a critical gap in the cybersecurity literature by determining how cognitive load and urgency traps hinder employee cybersecurity behavior in hybrid work environments. Specifically, three related research questions will be addressed. The first research question will examine how work overload in hybrid environments affects employees' ability to deploy cognitive resources when

making secure decisions. Secondly, how does workplace telepressure affect the psychological mechanisms that influence employee cybersecurity behavior? Finally, what organizational interventions can be implemented to reduce cognitive load without blaming employees?

This research will focus on understanding the environmental and systemic factors that influence security, rather than blaming individual employees for their lack of security. It will lay the foundation for creating human-centered security solutions that account for today's organizational workload realities. In addition, the research will evaluate the intersection of cognitive demand, telepressure, organizational identification, and cybersecurity behavior by employing research studies conducted from 2020 to 2025. As well, research across organizational psychology, neurocybersecurity, and behavioral cybersecurity has produced substantial empirical work on this topic (Kritika, 2025; Kim et al., 2024).

This research will have immense implications for organizations, cybersecurity practitioners, and researchers. By understanding these dynamics, organizations can develop and deliver security solutions that account for the cognitive constraints of human resources and the effects of environmental stressors. For security practitioners, this research will guide the design and delivery of evidence-based security interventions that enable appropriate secure behaviors. For researchers, this research will contribute to the continued development of literature that moves away from deficit-based models of human security behavior and calls for interventions at the systemic and organizational levels (Aschwanden et al., 2024).

Theoretical Framework

Cognitive Load Theory and Security Decision-Making

Sweller developed Cognitive Load Theory (CLT) as a basic framework for conceptualizing how limitations in processing information affect how we learn and make decisions. CLT holds that our working memory has limited capacity and that exceeding it leads to rapid performance decline. The implications of cognitive load in a cybersecurity environment are significant because the limitations of working memory affect our ability to assess multiple variables simultaneously, recognize patterns, and evaluate risk - all of which place a very high cognitive demand (Kritika, 2025).

The application of CLT to employees' behavior in cybersecurity highlights that employees face three types of cognitive load when making security decisions. The first type of cognitive load is intrinsic, referring to the complexity of security tasks and the identification of security threats. Cyber threats are increasingly using advanced social engineering techniques that closely mimic legitimate communications. Therefore, employees must carefully examine their communications to identify and investigate subtle indicators of compromise (Aschwanden et al., 2024). The second type of cognitive load is extraneous, which occurs when the security interface is poorly designed, difficult to authenticate, or has policies that are too confusing, increasing the cognitive burden of understanding and complying with security policies without increasing employees' security knowledge. The third type of cognitive load is germane, which involves the cognitive resources dedicated to developing or expanding cognitive schemas and recognizing patterns that help employees identify and respond to security threats (Kritika, 2025).

Research has shown that cognitive overload can impair an employee's ability to make security decisions in several significant ways. When the employee's cognitive load is high, he/she is more likely to use automatic, heuristic-based decision-making rather than thoughtful, analytical processes to make security decisions. This is the activation of what Dual-Process Theory describes as Intuitive thinking, or fast, automatic, and subject to cognitive biases, and the suppression of Reasoning thinking, which is slow, structured, and analytical. Threat actors exploit the natural tendency of individuals to act on initial assessments of their environment. They create attacks that appear legitimate on their face so that automatic responses occur before analytical processing identifies a threat (Kritika, 2025).

Cognitive load challenges are significantly higher in a hybrid working environment, as employees are required to constantly switch between work and personal domains, manage communications across multiple platforms, and address security concerns across various digital environments (Cambier & Vlerick, 2022). Each time an

employee switches contexts, this imposes a "switching cost" that reduces cognitive capacity and creates windows of vulnerability to social engineering attacks, making employees more susceptible (He et al., 2024). In addition, employees' continuous availability expectations in a hybrid work environment create a state of partial attention, forcing them to monitor multiple sources of information simultaneously without fully concentrating on any single task (Cambier & Vlerick, 2022).

Empirical evidence exists that demonstrates the relationship between cognitive load and cyberspace behavior. For example, several studies have analyzed an individual's susceptibility to phishing, indicating that individuals under time pressure and/or cognitive load exhibit a significantly higher rate of phishing emails than in control conditions. Similarly, many researchers have examined how individuals behave concerning passwords. As cognitive resources were depleted by demanding tasks, individuals selected weaker passwords and displayed poorer password hygiene (Aschwanden et al., 2024). Based on these findings, the authors believe that secure behavior is not merely dependent on knowledge and/or intention, but rather fundamentally depends on the availability of cognitive resources at the time of decision-making (Kim et al., 2024). The implications of CLT for understanding the "Urgency Trap" are evident in how threat actors design attacks. Deliberate time pressure and urgency are common tactics in sophisticated social engineering attacks (Aschwanden et al., 2024). The use of urgent deadlines creates cognitive overload by triggering a sense of urgency, along with emotional appeals and perceived authority, so that the victim cannot assess potential threats. This exploitation of human cognitive limitations shows that employees cannot be viewed as the weakest link. Instead, the organizational systems that put them in a position to assess threats are the issue (Kim et al., 2024).

Protection Motivation Theory and Cybersecurity Behavior

Protection Motivation Theory (PMT) has its origins in Rogers' work, providing an additional framework for understanding how people react to security threats, and has been modified to include information security. PMT states that an individual's cybersecurity behavior is based on two cognitive functions: a threat appraisal, which considers the perceived likelihood and severity of the threat, and a coping appraisal, which evaluates the self-efficacy and response-efficacy of available behaviors.

There are many examples in the literature that have used PMT to relate to compliance with security policies, awareness of protective measure behaviors, and the likelihood of implementing those behaviors, among others. As PMT specifies, if people perceive the threat as severe, are considered vulnerable, possess response

efficacy, and believe they can implement the behaviors, they are likely to adopt behaviors to enhance their security. However, PMT has an underlying assumption: that people have sufficient cognitive resources to perform threat appraisal and coping evaluation (Kritika, 2025). Regarding the integration of PMT and cognitive load principles, there are substantial deficiencies in traditional security awareness initiatives, which primarily aim to enhance threat awareness and instruct employees on implementing protective actions, thereby fulfilling the threat appraisal and response efficacy elements of PMT (Aschwanden et al., 2024). However, such intervention is ineffective when employees lack the cognitive resources to apply the learnt material in a real-world threat situation. The "Urgency Trap" severely compromises the individual's ability to conduct an adequate coping appraisal of an identified threat, placing them in a situation in which they recognize an existing threat but lack the time and ability to implement protective action (Cambier & Vlerick, 2022).

Studies of workplace telepressure, for example, have demonstrated that hybrid work environments, in general, create systematic conditions that prevent individuals from successfully implementing the components of PMT to motivate effective defensive behavior. Individuals who work in such environments and experience elevated levels of telepressure are more prone to making security-related decisions impulsively (e.g., clicking a suspicious link or sharing their credentials) than those who do not experience telepressure. However, this impulsive behavior is not indicative of a lack of security knowledge. Instead, the urgency of work dictates that impulsive decisions take precedence over deliberate security-based decision-making (He et al., 2024). In this regard, telepressure challenges the assumption that security awareness alone is sufficient to enable secure behavior. Therefore, in addition to motivation and capability, sufficient cognitive resources are required to drive secure behavior (Kim et al., 2024).

Moreover, PMT's self-efficacy component is highly relevant in the hybrid work environment. Self-efficacy refers to the individual's belief in their ability to execute a given behavior successfully. Thus, it encompasses the potential for technology to buffer the negative impact of workload on workplace security behavior (Kim et al., 2024). Self-assured employees do not correlate work burdens with the number of safety/security failures when using AI. This means that the employee's use of technology will not be solely responsible for the adverse outcomes of AI use. Also, any cognitive lapse will now shift some responsibility for adverse outcomes onto the organization and its technological support systems (Kritika, 2025).

PMT's definition of response costs becomes especially pertinent under circumstances of cognitive overload. Response costs are defined as the effort, time, and inconvenience an employee experiences when complying with a security

procedure. Therefore, a worker, given their cognitive capacity, can reasonably deal with an elevated response cost while perceiving a higher-than-normal threat. However, when workers are overwhelmed and trapped in the "Urgency Trap", it will be difficult for them to comply with procedures when even minimal responses are perceived as too costly and impede compliance. Because of cognitive overload, employees will not willingly contravene security processes. They do so because compliance is challenging under time constraints (Aschwanden et al., 2024).

Applying PMT to a hybrid work environment illustrates that employee security behavior results from threat perception, coping ability, and the availability of cognitive resources. Previous security practices that have placed accountability for the organization's safety solely on employees have assumed that employees possess unlimited cognitive capacity. This is not true of most current work environments. Thus, security must consider employees' cognitive limitations to support the organization and encourage them to act securely (Kim et al., 2024).

As integrated perspectives illustrate three main ways that hybrid environments negatively impact cybersecurity:

1. Excessive cognitive loads created by work overload and telepressure impede employees from identifying and assessing threats.

2. The "Urgency Trap" utilizes unconscious decision-making processes, or automaticity, which can be exploited in social engineering attempts.

3. Continuous connectedness creates chronic stress and diminishes organizational identification and motivation for security, leading to a psychological disconnect from responsibility for security behaviors (He et al., 2024).

Ultimately, this dual approach explains that traditional security systems fail. Security awareness training provides employees with the information they need, but does nothing to reduce their cognitive load. Security policies outline expected outcomes but do not provide the cognitive resources needed to comply. Technical controls reduce some security decision-making. However, employees must exercise judgment when making security decisions under uncertain circumstances (Aschwanden et al., 2024). Security in the hybrid work environment must employ interventions that target cognitive and motivational influences driving insecure behaviors rather than their manifestations (Kim et al., 2024).

Empirical Evidence

Study 1: Workplace Pressure and Employees' Behavior

This study aimed to examine the association between workplace pressure and employees' behavior beyond their work hours, and vice versa (Cambier & Vlerick, 2022). To assess this relationship, a longitudinal diary study design with three points was utilized, and 269 full-time employees were asked to complete daily diaries for five consecutive days. There were 1,256 diary entries. This design provided a means to examine fluctuations in workplace pressure and behavior within individuals, as well as how daily variations in cognitive states affected their behavior.

The operational definition of workplace pressure in this study is the preoccupation and urge to respond immediately to work-related information outside of work (Cambier & Vlerick, 2022). It is measured by six items from the Workplace Telepressure Measure. Message-based communication behavior was measured through self-report measures of the frequency of sending and checking work messages while at leisure. Affective rumination at work was measured using five modified items from the Work-Related Rumination Questionnaire. To examine the specific relationship between workplace telepressure and affective rumination, daily levels of stress and work activity were included as covariates.

Multilevel modeling was used to assess the relationship between workplace telepressure during leisure time and its effect on affective rumination toward work. Daily telepressure during leisure time positively predicted affective rumination about work issues. Telepressure's influence on affective rumination was also found to be mediated by message-based communication behaviors, indicating that workplace telepressure elicits specific communication behaviors, which in turn produce affectively negative, intrusive thoughts about your work, providing support for complete mediation between workplace telepressure and affective rumination through communication behavior.

Additionally, this study has clearly shown that there are bidirectional effects in boundary-crossing contexts. Affective rumination about private issues at work was similarly affected by telepressure stemming from their private lives (i.e., personal messages) through one's communication behavior toward these messages, which were also experienced at work. These two findings demonstrate that hybrid work (due to boundary permeability) creates bi-directional cognitive drains, thereby preventing employees from obtaining adequate psychological detachment from their work and personal lives, which is critical for cognitive recovery. (Cambier & Vlerick, 2022).

The contribution of this study to theory is how the telepressure-induced communicative behaviors that establish resource-depleting experiences result

in affective rumination in both occupational boundary-pushing contexts. This contradicts the assumption that a quick or timely response to a work-related message after hours is a non-obtrusive interruption. Instead, with each interaction through work-related messages, the individual's work-related cognitive schema is activated, thereby preventing the necessary psychological detachment from their occupational duties. Hence, individuals are unable to engage in cognitive recovery and replenish their cognitive resources necessary to deal with stress-related issues (Cambier & Vlerick, 2022). The chronic depletion of these cognitive resources has an accumulative effect over time. It leaves employees without the cognitive resources to make reasonable decisions, including cybersecurity-related decisions.

The cybersecurity implications of workplace telepressure are significant because employees who experience it continually have their cognitive resources committed and, as a result, do not possess the concentration and cognitive resources necessary for effective threat detection, i.e., identifying the characteristics of social engineering attacks. Social engineering attacks that occur after hours target employees while they are in a depleted cognitive state, making it difficult for them to appropriately analyze email content before acting. Additionally, the urgency that employees feel due to telepressure is what many sophisticated phishing attacks exploit-they apply pressure on employees to respond immediately, without allowing them time to verify the authenticity of the email (Cambier & Vlerick, 2022).

Study 2: Work Overload, Organizational Identification, and Cybersecurity Behavior

To investigate whether an imbalance between job demands and employees' available resources negatively affects cybersecurity behaviors, Kim et al. (2024) conducted a diverse, three-wave longitudinal study involving 410 participants from multiple industries in South Korea. To minimize the likelihood of standard-method variance, they measured the predictors, mediators, and outcomes at three different points in time, thereby establishing an acceptable temporal order among the variables that support causation.

The authors defined work overload as employees' perceptions that they have insufficient resources to meet the demands of their jobs effectively. Cybersecurity behaviors included employees' levels of vigilance in identifying threats, their adherence to organizational cybersecurity protocols, and their proactivity in engaging in security-oriented behaviors (Kim et al., 2024). The authors assessed job stress using well-validated, objective measures of psychological stress and organizational identification, namely, employees' feelings of connection with their organization. A structural equation model that included job stress and organizational

identification as sequential mediators of the relationship between work overload and cybersecurity behavior was assessed, controlling for demographic variables (e.g., age, gender, education, and job level).

The analysis findings support the hypothesis that excessive job demands negatively impact cybersecurity behavior (Kim et al., 2024). Moreover, the data indicate a sequential relationship in which work overload increases job stress, which, in turn, reduces employees' sense of identification with the organization. Additionally, because of their reduced identification with the organization, employees exhibit poorer cybersecurity behaviors. The indirect effect of work overload on cybersecurity behavior, mediated by both job stress and organizational identification, was statistically significant, thereby supporting the sequential mediation hypothesis (Kim et al., 2024).

An additional significant contribution of the study to the causal mechanisms underlying work overload, job stress, and organizational identification in predicting cybersecurity behavior is the introduction of AI self-efficacy as a moderating factor between independent and dependent variables. Studies showed that self-efficacy in AI use significantly reduced the positive impact of work overload on job stress (Kim et al., 2024). Work overload significantly reduced the effect of work stress on job stress among those with high self-efficacy in using AI, suggesting that self-efficacy serves as a cognitive buffer against the adverse effects of work overload. These findings challenge previous cybersecurity research, which relied solely on human-centered approaches, and show that providing the appropriate level of technological enhancement can help address human cognitive limitations.

The organizational identification pathway was identified as an important psychological mechanism that reduces security within organizations due to work overload. When employees are overworked and experience chronic stress from excessive demands, their psychological attachment to their organization diminishes (Kim et al., 2024). As a result, diminished attachment will lead to reduced intrinsic motivation to protect organizational assets, thereby shifting security from a valued responsibility to an additional burden. This aligns with the finding that individual responsibility of security organizations is less important, as organizational factors, including design, resource allocation, and employee stress management, play a direct role in determining the security outcomes of organizations through their effects on employee motivation and psychological attachment to the organization (Kim et al., 2024).

The research's focus on work overload as a chronic, systemic issue rather than an individual problem represents a fundamental shift in how cybersecurity is studied. Traditionally, security failures were generally perceived as the result of a

lack of knowledge or negligence. This research demonstrates that when the work environment causes significant cognitive and emotional overload to a knowledgeable and willing employee, the employee develops poor security behaviors. Therefore, to improve security within organizations, organizational design and conditions must be improved, and not simply by providing training for individual employees or implementing more stringent controls.

Study 3: Cognitive Biases and Cybersecurity Behavior in Enterprises

Aschwanden et al. (2024) conducted a study to examine how cognitive biases influence cybersecurity behavior in medium- and small-sized businesses. This research used qualitative methodologies. Qualitative analysis was conducted through structured in-depth interviews with 44 participants, including employees, decision-makers, and IT service providers from these organizations. Three unique personas with distinct cognitive biases regarding cyber risks were identified. Utilizing this persona-based framework, the research provides unique insights into the psychological mechanisms driving individuals' insecure actions.

The expert persona consists of those who possess self-confidence in their cybersecurity concepts but exhibit two notable cognitive biases. The first bias is overconfidence bias, in which the expert overestimates their ability to handle a risk and underestimates it, leading them to fail to take adequate preventive measures, even though they are aware of the risk (Aschwanden et al., 2024). The second bias captured within the expert persona is the intention-behavior gap: while experts possess the knowledge and intent to perform securely, they fail to do so due to one of three factors: time perception, convenience, or perceived effort. This research finds that experts over-rely on IT service providers to manage their cybersecurity and do not adequately understand the behavioral vulnerabilities associated with cybersecurity (Aschwanden et al., 2024).

The deportee persona comprises individuals who have deferred their cybersecurity responsibilities or accountability to others, typically to IT service providers. Because of their lack of cybersecurity expertise, individuals in this persona exhibit the bystander effect and diffusion of responsibility (Aschwanden et al., 2024). Individuals in this persona believe there is someone else, usually the IT department, who is responsible for preventing and addressing breaches. This cognitive pattern has created vulnerabilities for organizations in terms of trust in employees' and decision-makers' behavior and in their decisions regarding behavioral security measures. Meanwhile, IT service providers have focused solely on technical solutions and lack the authority or capacity to effectively address behavioral aspects of security (Aschwanden et al., 2024).

The repressor persona describes individuals who tend toward cognitive dissonance and information avoidance regarding their perceptions of cyber risk. Such individuals hold erroneous beliefs that their organizations are low-value targets for cybercriminals, demonstrating both optimism bias and availability bias (Aschwanden et al., 2024). When presented with information about cyber risk, repressors demonstrate avoidance or dismissal, thereby reducing the cognitive dissonance associated with their insecure behaviors despite understanding that they should act differently. As many repressors have not experienced a cyberattack, they tend to underestimate the likelihood of their organization being attacked (Aschwanden et al., 2024).

This theoretical contribution identifies that people must be provided with tailored interventions that address each person's unique cognitive biases. Individuals who are characterized as experts should receive interventions to reduce overconfidence through margin-of-safety planning, to create habits through automatic reminders, and to provide action plan development with clear implementation intentions (Aschwanden et al., 2024). In contrast, individuals who are classified as deportees should receive interventions to clarify the boundaries of responsibility, thereby creating normative expectations for security-related behaviors that will help eliminate diffusion of responsibility. Lastly, individuals who exhibit the repressor persona should receive experiential interventions, such as simulated cyberattacks on their organization, to counteract their information avoidance and crystallize the tangible, immediate nature of their cyber risk.

From a cognitive load perspective, the research shows that cognitive biases serve a functional purpose: they reduce cognitive load and allow for immediate decision-making without extensive analysis. However, in cybersecurity, cognitive biases create vulnerabilities that cybercriminals can exploit. The Cognitive Load Theory states that the "Urgency Trap" exacerbates cognitive biases by imposing time pressure that impedes analytical processing, thereby increasing reliance on cognitive shortcuts (i.e., heuristics). Focusing on the cognitive bias patterns identified in the research can lead to interventions that complement cognitive tendencies, thereby reducing cognitive load rather than adding to it.

The context examined shows that computer security issues do not exist only in large companies with dedicated security professionals. Instead, many small- and mid-sized businesses may lack the resources to develop comprehensive security programs, making the cognitive and behavioral components of computer security much more important to them (Aschwanden et al., 2024). The conclusion that diffusion of responsibility leads to an underdeveloped state of implementation of behavioral computer security indicates that there is an organizational systemic problem, rather than a personal deficiency, related to adequate computer

security (Aschwanden et al., 2024). To effectively implement computer security, an organization will require not only technical means but also clearly delineated organizational structures with established responsibilities and support systems to ensure organizational members' adherence to computer security countermeasures (Aschwanden et al., 2024).

Developing Interventions

To address the cognitive and structural mistakes inherent in the "Urgency Trap," which is not a matter of morality, simply adding more training will not resolve this issue. Traditional security awareness training only perpetuates the problem by exhausting users' cognitive load and increasing their cognitive burden. To create a resilient environment for hybrid workers who experience high levels of cognitive overload, a recommitment to the study of social psychology and cognitive ergonomics is required when approaching cybersecurity. The interventions described below suggest a shift toward a Human-Centric Zero Trust Architecture (ZTA) supported by AI self-efficacy and grounded in psychological safety (Aschwanden et al., 2024; Kritika, 2025; Kim et al., 2024; Rose et al., 2020).

Human-Centric Zero Trust: De-burdening the User

ZTA is the modern industry standard for cybersecurity. ZTA has always been defined as "never trust, always verify," and is too frequently misconstrued as a suspicion-based approach toward employees (Rose et al., 2020). However, viewed through the lens of Cognitive Load Theory, ZTA offers a significant psychological benefit by relieving the user's overloaded working memory of the burden of making trust-based decisions. Under a legacy perimeter security model, once an individual/user enters through the perimeter, they enjoy the implicit benefit of being trusted. This creates a significant cognitive burden on that employee/user to avoid losing their trust by, for example, clicking on the wrong link or downloading the wrong file. The employee/user is, in essence, acting as the gatekeeper to the enterprise, making significant trust-based decisions by virtue of having created an implicit agreement (for lack of a better description) between themselves and the enterprise. Under ZTA, there is "no implicit trust" granted to any asset or user account solely based on physical or network location (Rose et al., 2020). Authentication and authorization are two distinct processes that are performed at regular intervals (i.e., per session) during a user's session to help reduce the burden of constantly having to keep track of whether what they are doing is safe or not (Rose et al., 2020; Kritika, 2025; Aschwanden et al., 2024).

This paper suggests that ZTA should be implemented as a cognitive offloading technique, rather than a control method, by automating the processes associated with verifying whether the user's device is in an appropriate posture (e.g., correctly configured), consistently authenticating the user to the device, and using behavioral analytics to make decisions regarding the user accessing their device. Thus, the user would no longer have to continuously ask him/herself, "Is this safe or not?" because the architecture will automatically treat access requests as unsafe until the

architecture can demonstrate otherwise (as opposed to waiting for a human to make that determination) (Rose et al., 2020). According to Rose et al. (2020), the Trust Algorithm integrated into the ZTA policy engines evaluates access requests against multiple inputs, including subject identity, asset status, and threat intelligence, and establishes a dynamic level of trust before granting access to the requesting party. All of this is accomplished through computational means and provides a buffer between the user and the burden of making security-related decisions.

The use of ZTA as proposed in this paper can be easily achieved using currently available Identity and Access Management platforms and Secure Access Service Edge architectures, thereby making this approach highly feasible. Furthermore, it is more ethical than legacy models because it removes the burden of security-related decisions from employees, who will inevitably make mistakes when relying on ZTA to make the same decisions. In addition, by implementing ZTA in this manner, the accountability for security-related decisions has been transferred from the user to the ZTA framework via the following ZTA principle: "Access to resources is determined by dynamic policy — including the observable state of the client identity, application/service, and requesting asset — and may include other behavioral and environmental attributes" (Rose et al., 2020), resulting in the verification of user access requests being accomplished systematically, rather than relying on user vigilance.

The Protection Motivation Theory suggests that using this intervention will reduce the cost of recovery from a cybersecurity incident (e.g., time away from work and the effort required to "be secure"). Employees will not expend effort to ensure their own security. The system enforces it. The intervention also prevents deportee bias (Aschwanden et al., 2024), the tendency to shift the burden of cybersecurity onto IT service providers (i.e., "that is IT's responsibility"). While instituting the "IT handles it" mentality under Human-Centric ZTA is indeed secure rather than negligent, the architecture will support employees' cognitive limitations by automating most routine security decisions through the use of policy enforcement points and policy engines, while providing opportunities for continuous verification (Rose et al., 2020; Aschwanden et al., 2024; Kim et al., 2024).

Enhanced cognitive flexibility through AI self-efficacy

One interesting proposition derived from the literature is that cognitive overload could be mitigated through increased awareness of one's ability to use AI. Kim et al. (2024) demonstrated that employees who were confident in their ability to use AI exhibited much lower levels of job stress and engaged in more desirable cybersecurity behavior, because higher levels of self-efficacy in AI use significantly weakened the positive relationship between work overload and job stress. This

finding presents a new avenue: AI could not only be deployed to detect threats to an organization, but also to enhance an employee's ability to process information (Kim et al., 2024).

Organizations should provide AI-assisted co-pilots to help filter out the "Urgency Trap". These will provide employees with tools to triage communication into truly urgent and non-urgent categories, reducing some of the Extraneous load associated with the techno-invasion many workers experience in hybrid or remote work environments (He et al., 2024; Cambier & Vlerick, 2022). As such, an organization will need to provide staff with instructions on how to use these AI applications to assist with workload management. Kim et al. (2024) demonstrated that when employees develop their AI skills, they become more confident in their ability to use these technologies effectively, thereby minimizing the negative impacts of excessive work on job-related stress. It is also recommended that the training be delivered through scenarios that occur within employees' regular workflow, following gamification principles to reduce unnecessary cognitive load (Kritika, 2025).

The conventional view is that all cognitive loads are bad. However, if cognitive resources are appropriately allocated to schema development and pattern recognition (Germane load), this can increase cognitive flexibility. The use of artificial intelligence to automate repetitive tasks (Extraneous load) will allow organizations to free up their users' cognitive resources for more complex problem-solving (Germane load) (Kritika, 2025). This increased cognitive flexibility will help employees be more adaptable and resilient to new social engineering attacks that rely on critical thinking rather than compliance processes (Aschwanden et al., 2024). Gamified training interventions, based on the principles of Cognitive Load Theory, that use visual feedback, stories, and scenarios can further reduce the Extraneous load an employee may experience while simultaneously enhancing the Germane load (Kritika, 2025).

This intervention focuses on the root of the "Urgency Trap" and removes distractions that prevent employees from focusing on their jobs. By filtering out interruptions, an organization enables its users to refocus. A high level of self-efficacy regarding artificial intelligence can help buffer against employee burnout by providing cognitive resources to complete threat assessments (Kim et al., 2024). As Kim et al. (2024) stressed, organizations should strategically channel AI technologies to reduce work overload and increase cybersecurity, just as we should employ them to automate repetitive tasks.

The "Anti-Telepressure" Policy: Changing Norms

Psychological interventions should be designed to counter the organizational norms that lead individuals to feel telepressured. According to He et al. (2024), the perception of reward for responding to work-related messages after hours is a significant moderator of the association between task interdependence and workplace telepressure. This implies that when individuals perceive they will receive a greater reward for responding to work messages after hours, the association between work-related demands and telepressure will increase. The "Urgency Trap" is therefore treated as a financially incentivized relationship. As a result, speed must be separated from value (He et al., 2024).

To change telepressure-inducing norms and behaviors, organizations should implement "Asynchronous by Default" communication policies. This means leaders must model acceptable behavior and prioritize long-term over short-term outcomes. He et al. (2024) suggested organizations should "reduce rewards for processing work tasks during nonworking hours, and increase rewards for effectively completing work during working hours". Furthermore, clarify that employees will not be mistreated or evaluated poorly for failing to respond to work-related messages after hours, nor will they be given preferential treatment for responding to such messages after hours (He et al., 2024). They also clarified that employees would not receive favorable performance reviews for responding to work-related messages after hours (He et al., 2024). This also directly counters the "boundary condition" outlined in their study, which holds that affirming self-worth through others strengthens the relationship between dispositional anxiety in the workplace and workplace telepressure (He et al., 2024).

Behavioral nudges derived from behavioral economics research can reduce telepressure by prompting users to communicate outside of business hours. For example, the email program can prompt the user by stating, "You are sending this email at 9 PM. Do you wish to schedule delivery for 8 AM tomorrow?" This prompt disrupts the automatic urgency or Intuitive Thinking behavior and engages both levels, including Rational Thinking.

Rather than using gamification to encourage employees to respond quickly to work-related communications, organizations should use it to foster Rational Thinking. For example, organizations could use gamification platforms to reward employees who report phishing emails or identify process vulnerabilities (Kritika, 2025). This creates a self-determination theory sense of competence ("I can identify threats") and autonomy ("I can protect my organization") rather than reinforcing telepressure behaviors. By creating a gamification-style security experience, organizations can induce a flow state in users. As a result, users' cognitive focus is on the threat rather than distractions (Cambier & Vlerick, 2022). Cambier & Vlerick (2022) stated that

telepressure-driven communication behavior is a resource-depleting experience that creates affective rumination (stress) in cross-boundary communication contexts. Therefore, reducing rumination by reframing norms increases both employees' well-being and the cognitive resources available to identify possible threats (Cambier & Vlerick, 2022).

Customized Approaches Based on Personas

Recognizing that not all users are the same, Aschwanden et al.'s (2024) research can help create custom solutions for different personas. A universal approach implies that each person's cognitive distortion will not be addressed. The study by Aschwanden et al. (2024) states that there are three persona types (expert, deported, and repressed) with distinct cognitive biases, each requiring distinct solutions.

Table 1

Customized Approaches Based on Personas

Persona	Cognitive Biases	Customized Solution
The Expert	Overconfidence bias; Intention-behavior gap (Aschwanden et al., 2024)	Do not provide any basic training, as this could lead to inflated self-perception. Encourage participation in "Red Team" exercises or "IKEA effect" - type exercises that help develop security rules. By participating in the development of goals for cyber and identifying unsafe activities (i.e., shared passwords or passwords that are not changed), they (Experts) will have a higher level of adherence to the outcome (Aschwanden et al., 2024). Creating habits through automatic reminders and planning specific implementation steps can close the intention-behavior gap.

Persona	Cognitive Biases	Customized Solution
The Deportee	Diffusion of Responsibility; Bystander effect (Aschwanden et al., 2024)	Create an environment of invisible security by using a Human-Centric Zero Trust Architecture and a high level of automation in the enforcement process, so that the deportees feel as if, by "letting IT" do it, it has truly been done (Rose et al., 2020). Using defined "contracts" to specify who is responsible for what (the deported person for physical security and the IT department for IT Security) will provide clarity and define where the responsibility lies. By using frequent messages and education to help reduce the likelihood of bystander behavior (Aschwanden et al., 2024).
The Repressor	Optimism bias; Availability bias; Avoidance of information (Aschwanden et al., 2024)	"Internally initiated safe attacks" (simulations) can help change the repressor's optimism bias by demonstrating how easily others can be deceived safely, forcing them to re-evaluate their vulnerability without causing any harm (Aschwanden et al., 2024). Provide examples of current cyberattacks targeting similar businesses to help the repressor perceive risk through the availability heuristic. Gamified techniques increase motivation and reduce information avoidance by making risk tangible (Kritika, 2025).

As a method for influencing the behavior of all cyber experts, the COM-B (Capability, Opportunity, Motivation) model of behavior change indicates that experts possess the psychological capability and reflective motivation to comply with cybersecurity behaviors.

However, experts do not have automatic motivation or social opportunities to engage in cybersecurity behaviors (Aschwanden et al., 2024). To motivate compliance, establish team goals (e.g., a score with zero tolerance) after all team members have contributed to their establishment (Aschwanden et al., 2024).

The key issue facing deported individuals is the lack of a single individual feeling responsible for the behavioral measure(s), as responsibility is continually passed back and forth (Aschwanden et al., 2024). This diffusion of responsibility can be addressed by establishing explicit contracts that define the responsibilities of the decision-maker and the IT service provider at the time of initial engagement (Aschwanden et al., 2024). The technological foundation of the Human-Centric ZTA discussed here provides the deportees with a means to automate what they want to offload to others (Rose et al., 2020).

Repressors must deal with cognitive dissonance by rationalizing the unsafe behavior(s) as their organization is too small or uninteresting for an attacker to attack. They do not realize that much of the motivation for cyberattacks comes from bots that systematically search for vulnerabilities (Aschwanden et al., 2024). Repressors can change their perception of risk by participating in simulated attacks and receiving immediate positive reinforcement for successfully identifying a threat (Aschwanden et al., 2024; Kritika, 2025). The fact that individuals under time constraints exhibit much higher rates of falling for phishing emails reinforces the importance of creating a safe, simulated environment in which repressor individuals can experience vulnerability without real-world consequences.

The Role of Corporate Ethics

The intervention framework should be integrated into an ethical corporate culture. Kim et al. (2024) demonstrated that organizational identification is a vital mediating factor in the relationship between working conditions and security behaviors. When individuals experience chronic stress due to high workloads, their connection to their employers weakens, thereby affecting their ability to behave securely. Companies with an ethical culture that prioritizes the fair treatment of employees (i.e., protecting their time and valuing their health) provide a buffer against the stress that drives security workaround behaviors (Kim et al., 2024).

If there is a sense of trust between employees and the organization (i.e., high

organizational identification) regarding employee well-being, employees will not utilize "fear control" measures when they face a security problem. However, they will instead employ "danger control" strategies, proactive rather than avoidance (Kim et al., 2024). Developing a sense of identification will require demonstrating a commitment to employee well-being, providing resources and support for their security responsibilities, and fostering a security culture that values prevention over blame (Kim et al., 2024). Aschwanden et al. (2024) stated that interventions should "not represent additional barriers for the employees and decision makers, and, instead, they should be easy and fun to implement." When cyber security interventions are perceived as supportive rather than punitive, they reinforce the ethical foundation on which sustainable security behaviors are developed (Aschwanden et al., 2024; Kim et al., 2024).

Ethical Considerations and Implementation Challenges

Implementing human-centered security interventions raises many ethical considerations that warrant careful consideration. For example, the use of behavioral monitoring and artificial intelligence-enhanced security tools can raise privacy concerns due to employee surveillance. To meet legitimate security needs, organizations must respect employee privacy and implement transparent policies that detail what data will be collected, how it will be used, and the safeguards in place to prevent misuse. An ethical framework should focus on the need for informed consent, limitation of purpose, and employee involvement in the governance of the systems used for monitoring (Kritika, 2025).

Another ethical issue is the potential for gamification and various behavior-based interventions to manipulate employees in an ethically objectionable manner. Nudge-based interventions influence behavior without the individual's explicit awareness, thereby undermining their autonomy and ability to make informed decisions about their security. Ethical gamification requires the designer to provide transparency regarding the elements of persuasive design that may influence the individual. Therefore, gamification should support, rather than replace, a genuine understanding of security (Kritika, 2025). The goal of an ethical approach to gamification is to enable individuals to make informed security decisions, rather than to manipulate behavior through psychologically based techniques unbeknownst to them.

The third consideration is that interventions that reduce individual cognitive load through automation or organizational support should not lead individuals to develop learned helplessness or the belief that they have abrogated all security responsibilities (Aschwanden et al., 2024). They should also seek to strike the right balance between aiding and developing capabilities so that they help the individual

make a secure judgment. For example, if an organization uses AI-based systems for threat detection, it should ensure that the systems explain their reasoning to users so that users can develop their own pattern recognition capabilities and avoid reliance on the automated system (Kritika, 2025).

Organizations will also face numerous practical issues in implementing the above ethical considerations. Cultural change is a slow process that requires ongoing effort and commitment from leaders, as it is not feasible to establish a security culture through policy alone (Aschwanden et al., 2024). Small and mid-sized organizations may be limited in their ability to implement the sophisticated technical interventions discussed above due to limited resources (Aschwanden et al., 2024). However, many non-technical organizational interventions (such as more straightforward assignment of responsibilities, better management of employee workloads, and more precise boundaries) typically require very few resources. They can have a high impact, especially when organizations have limited technical controls (Aschwanden et al., 2024). Measuring the success of various interventions poses an additional challenge for organizations, as improvements in security may be inferred from the absence of incidents (Kim et al., 2024). Therefore, organizations should employ multiple measures, including leading indicators (e.g., compliance with security-related behaviors, rate of identification of possible threats) and cultural indicators/ employee-based measures (e.g., self-efficacy of employees related to security, employees' identification with the organization), along with the traditional lagging indicators (e.g., frequency and severity of incidents) to measure their success(Kritika, 2025; Kim et al., 2024).

Conclusion

This study challenges the widely held belief that "humans are the weakest link" in cybersecurity and concludes that this view is both an incorrect theoretical premise and results in underperformance in practice. This research continues to explore empirical literature using studies that span 2020 to 2025, and demonstrates that employees are not, through their inherent characteristics, weak security actors, but rather act as cognitive agents that are functioning under conditions characterized by extensive depletion of resources and a complex set of systemic constraints arising from modern-day hybrid working environments (Aschwanden et al., 2024).

The integration of two theories, Cognitive Load Theory and Defense Motivation Theory, provides insights into how work-related telepressure and work-related overload generate what is recognized as the "Urgency Trap" - the intersection of time pressure, cognitive depletion, and insufficient organizational expectations that collectively erode the security-related behaviors of employees (Cambier & Vlerick, 2022). Cognitive Load Theory establishes that humans' working memory is limited,

and that these limitations affect decision-making quality and increase reliance on cognitive shortcuts, which are susceptible to social engineering when multiple demands exceed cognitive workloads and/or approximate continuous connectivity. The Defense Motivation Theory establishes that, even with an understanding of threat and knowledge of risk-avoiding behaviors, the likelihood of enacting them is overwhelmingly determined by the availability of cognitive resources and the complementary structures of organizational support - structures commonly lacking in today's workplace environments.

The synthesis of existing empirical evidence supports three specific findings. First, telepressure experienced by employees during their non-working hours produces bidirectional cognitive depletion, resulting in a deficiency in attention and cognitive capacity, especially in threat recognition, because the employee's work and personal domains do not provide an environment conducive to psychological detachment (Cambier & Vlerick, 2022). The second conclusion is that when employees are under heavy workloads, it negatively influences their cybersecurity behavior through a chain of events: increased job stress leads to decreased organizational identification. This indicates that security deficiencies can result from systemic organizational failures rather than from an individual failing to meet expectations (Kim et al., 2024). The third conclusion is that the same group of cognitive biases (e.g., overconfidence, responsibility diffusion, and optimism bias) manifests within different communities of employees on a continuum and thus requires tailored interventions that address each community's unique psychological profiles and not just a "one size fits all" awareness approach (Aschwanden et al, 2024).

Social Psychology's application to understanding cybersecurity challenges can empower organizations by shifting their focus from identifying individual deficits to identifying the systemic conditions that support/enable secure behavior or inhibit/turn off secure behavior. This demonstrates that securing an organization is not strictly a technical problem that requires technical solutions, nor solely a human problem requiring increased training, but in actuality an organizational design problem requiring alignment between the supporting structures (workplace), demands of work (workload), and cognitive capabilities of workers (Kim et al, 2024). In addition to highlighting the conditions of organizations, social psychology reveals how organizational contexts shape individual behaviors through cognitive load, motivation, group norms, and identity processes - none of which are addressed through either traditional training interventions or traditional technical control methods (Aschwanden et al, 2024).

This understanding leads to several critical conclusions that inform interventions to increase organizational resilience by acknowledging the ongoing presence of cognitive overload. One primary focus of this discussion is that a human-centered Zero Trust architecture provides a framework for strict security controls

while minimizing the cognitive load on humans. Organizations using a Zero Trust framework will assume that cognitive overload is the normal state, will reduce security friction through the use of adaptive authentication and automated intelligence, and will provide contextual support to the individual at decision points to ensure the organization maintains security without placing undue cognitive demands upon the individual (Rose et al, 2020). Second, threat detection will improve through gamified, neuroplasticity-based neurocybersecurity methods, delivered via entertaining, flow-focused training that enables automatic identification and response to threats based on previously identified visual/digital/analogue patterns, even during cognitive overload (Kritika, 2025). Third, to sustainably improve cybersecurity behaviors, an organization needs to address the deep-rooted causes of poor cybersecurity behaviors, namely workload management, boundary creation, clearly defined responsibilities, and organizational identification (Kim et al., 2024).

The shift in cybersecurity philosophy is a notable change in practice. Moving from a paradigm in which the view of employees in an organization as the weakest link needing restriction and surveillance to one in which the view of employees in an organization as cognitive agents, warranting support and the correct conditions for achieving productivity, is a fundamentally different mindset about security (Aschwanden et al., 2024). This new perspective is based on the premise that security results from the interplay between individual capabilities, organizational factors, and technical systems, and that it does not reside in any single entity. Therefore, optimal security relies on a successful connection among these three components, not on the highest level of restriction for any one of them (Rose et al., 2020).

Several areas require ongoing research into cybersecurity. First, longitudinal studies examining the effects of cognitive overload on security behaviors would determine whether the observed effects are a temporary state or reflect gradual degradation of security behaviors (He et al., 2024). Second, cross-cultural studies on how various cultural contexts/organizational structures influence the relationship between workload and security behaviors will help establish the broader applicability of the research and identify culturally specific interventions (Aschwanden et al., 2024). It would be helpful if we had more data on how different approaches affect different organizations when aiming to achieve the best possible security outcomes while remaining practical within each organization's environment. The second step to achieving success through successful security initiatives is developing a better understanding of the effects that different types of cognitive or personality traits have on how an individual behaves towards security issues (i.e., possesses the capability to successfully interact with an organization's security rules and regulations, experiences of the organization, and other individual characteristics).

Next to developing a better understanding of how cognitive load affects employees' behavior towards security issues, awareness should also be developed regarding organizational culture and its effect on individuals' ability to complete security initiatives under stress (i.e., cognitive load; Aschwanden et al., 2024). Finally, identifying ways to restore individuals' decision-making capability regarding security after exposure to high cognitive load would help develop recommendations for determining optimal work limits/recovery periods (He et al., 2024).

The potential for implementing very real, measurable changes to the work environment for organizations that successfully implement successful security initiatives is considerable (Kim et al., 2024). Organizations must eliminate any barriers to the complete and proper execution of the processes that enable successful security initiatives. Organizations must develop a thorough understanding of their workforce's cognitive limits and overload in relation to security performance (Kim et al., 2024). The methods to accomplish this should include conducting workload studies to determine the limits of cognitive load versus cognitive restorative ability, and implementing and monitoring effective work/recovery boundaries (Kim et al., 2024) to create optimal working conditions for specific types of work (He et al., 2024). Cybersecurity professionals need to understand that implementing better security practices for themselves may require either increasing their numbers or reducing their workload, rather than adding new security obligations for staff already at maximum capacity (Kim et al., 2024). These two findings indicate that expertise in human factors is equally important as knowledge of technical aspects of security for those working in cybersecurity. When developing security policies and architectures, human factors analysis, usability testing, and cognitive task analysis should be integrated into evaluating how well security controls align with human cognitive abilities and work patterns (Aschwanden et al., 2024). When developing security awareness programs, attention should focus on skills for recognizing patterns and making decisions under duress, rather than just on providing information. Gamified and scenario-based approaches should help develop automatic threat recognition capabilities (Kritika, 2025). When conducting investigations into security incidents, investigators should focus on systemic and organizational issues that contributed to security failures rather than assigning blame to individuals (Aschwanden et al., 2024).

Policymakers and developers of security standards should develop frameworks that address human factors considerations. Security compliance standards mandating technical controls without regard for human cognitive limitations may create incentives for an employee to circumvent a control rather than implement it. As such, more effective standards would describe the desired security outcome without specifying how it would be achieved, based on the organizational context addressed by the employee. Additionally, standards should include organizational

practices that reduce cognitive overload for employees and support employee well-being as valid security expenditures (Kim et al., 2024).

In summary, this research demonstrates that the narrative of "humans are the greatest liability" is an overly simplistic appraisal of the cybersecurity challenges contemporary organizations face. Individual employees do not lack strength but lack systemic support and work under conditions of cognitive overload. Traditional training methods and technical controls cannot keep pace with the challenges of providing adequate employee support (Aschwanden et al., 2024). Hybrid work environments create "Urgency Traps" that exploit cognitive limitations by exerting both time and financial pressure, placing knowledgeable and motivated employees at risk of suffering from complex social engineering attacks (Cambier & Vlerick, 2022).

Cognitive load and defense motivation should constitute the central organizing principles for the design of effective cybersecurity in the contemporary environment. Acknowledging that secure behavior is a function of the availability of sufficient cognitive resources, the presence of supportive organizational conditions, and the provision of appropriately designed technical systems that enhance human capabilities, is critical (Kim et al., 2024). The transition from culpability-based approaches that view security failures as the result of individual moral failings to systemic approaches that recognize security as a by-product of well-organized sociotechnical systems is needed to validly assess the relative effectiveness of any security approach (Aschwanden et al., 2024).

To succeed, organizations must make significant changes to how they perform day-to-day activities, how they design security processes, and their research focus areas. The findings presented in this research clearly demonstrate the need for and ability to make such changes. By applying insights from social psychology, cognitive science, and organizational behavior to the cybersecurity domain, we can create programs that improve security while acknowledging human cognitive constraints (Kritika, 2025). The issue is not whether humans are the most significant liability, because they are not, but whether organizations will provide the support and conditions necessary for humans to succeed as the most significant asset (Aschwanden et al., 2024).

References

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behaviour: The psychological gateway for cyberattacks. Organizational Cybersecurity Journal Practice Process and People, 4(1), 32–50. https://doi.org/10.1108/ocj-02-2023-0004

Cambier, R., & Vlerick, P. (2022). When thoughts have no off switch: The cost of telepressure and message-based communication behaviour within boundary-crossing contexts. Occupational Health Science, 6(4), 545–564. https://doi.org/10.1007/s41542-022-00127-7

He, X., Gao, Q., Cao, Y., Bian, R., & Wang, X. (2024). "Always online": How and when task interdependence and dispositional workplace anxiety affect workplace telepressure after hours. PsyCh Journal, 13(4), 639-653. https://doi.org/10.1002/pchj.747

Kim, B., Kim, M., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behaviour: Highlighting self-efficacy in the realm of artificial intelligence. Current Psychology, 43(19), 17146–17162. https://doi.org/10.1007/s12144-024-05692-4

Kritika. (2025). A comprehensive review of gamification in neurocybersecurity. Journal of Cybersecurity Education Research and Practice, 2025(1), Article 13. https://doi.org/10.62915/2472-2707.1243

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication No. 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207