Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 16 (1), 2024
pp. 2043 - 2058

The impact of Philosophical Mindset and Work Overload on Cybersecurity Behavior based on the Role of Psychological Contract Breach, Burnout, and Self-efficacy in Interacting with Artificial Intelligence

Adineh Yazdani Khomeirani[1*]

1. M.Sc in clinical psychology, Khalkhal Branch, Islamic Azad University, Khalkhal, Iran.

Abstract

The present study was conducted with the aim of investigating the effect of philosophical mindset and workload on cybersecurity behavior based on the role of psychological contract violation, job burnout, and self-efficacy in interaction with artificial intelligence. To achieve the research objective, about 391 questionnaires were distributed and collected to collect the required information among managers and employees of knowledge-based companies. The information collected by the questionnaires was analyzed using SPSS24 and Smart PLS3 software using structural equation modeling. Also, to examine the quality of the measurement tool in this study, index reliability, convergent validity, and divergent validity were used. Analysis and review of the information collected from the research questionnaires using structural equation modeling showed that workload has a negative and significant effect on cybersecurity behavior. Workload has a positive and significant effect on psychological contract violation behavior. Workload has a positive and significant effect on job burnout. Workload has a negative and significant effect on self-efficacy in interaction with artificial intelligence. Philosophical mindset has a positive and significant effect on cybersecurity behavior. Philosophical mindset has a negative and significant effect on psychological contract breach behavior. Philosophical mindset has a negative and significant effect on job burnout. Philosophical mindset has a positive and significant effect on self-efficacy in interacting with AI. Psychological contract breach has a negative and significant effect on cybersecurity behavior. Job burnout has a negative and significant effect on cybersecurity behavior. Self-efficacy in interacting with AI has a positive and significant effect on cybersecurity behavior.

Keywords: Workload, Cybersecurity, Philosophical mindset, Psychological contract breach, Artificial Intelligence.

Received: 05 may 2024 **Accepted:** 22 June 2024 **Published:** 02 July 2024

Introduction

In a rapidly evolving digital landscape, organizations increasingly rely on technology to drive growth, innovation, and maintain competitive advantage. However, this growing dependence on digital systems has also exposed organizations to a wide range of cybersecurity threats. As a result, the importance of employee cybersecurity behavior, which refers to the actions and practices individuals take to protect their organization's computer systems, networks, and sensitive information from cyber threats, has become more critical than ever. In fact, research has shown that human error and negligence are among the leading causes of cybersecurity breaches, underscoring the need for organizations to prioritize employee cybersecurity behavior in their overall cybersecurity strategies (Kim and Kim, 2024).

A philosophical mindset, like a philosophical spirit, has characteristics that are evident in a person's behavior and mindset, in their interactions with others, in their approach to problems, and in all aspects of their lives, which distinguish them from others. A person with a high philosophical mindset is more likely to see problems in terms of long-term goals, creative generalizations, fundamental beliefs, and a wide range of logical choices. A person with a philosophical mind exhibits characteristics that can be grouped into three dimensions: comprehensiveness, depth, and flexibility. This person always strives to make his thoughts

comprehensive, sees problems in relation to a broad context and related to long-term goals, questions the obvious, and increases his chances of moving beyond ignorant prejudices, personal biases, and stereotypes. This person has the flexibility that comes with innovation, change, and creativity, and examines issues from multiple angles and aspects (Mohajiran et al., 2015). Therefore, a person with a high philosophical mindset is expected to have strong relationships and strong commitment. Understanding the impact of philosophical mindset on employees' cybersecurity behavior can help organizations design more effective strategies for training and raising awareness in the field of cybersecurity.

On the other hand, workload overload, which describes an individual's perception of an imbalance between job demands and their personal resources to cope with these demands, has emerged as a potentially key factor influencing employees' cybersecurity behavior (Bolling et al., 2015). As organizations face the challenges of the digital age, employees are often asked to take on more responsibilities and adapt to new technologies such as artificial intelligence (AI). The increasing prevalence of workload overload in today's organizations has become a critical issue, given its negative impact on employees' attitudes, perceptions, behaviors, well-being, and overall performance at work. For example, workload overload has been shown to negatively impact employees' job satisfaction, organizational commitment, self-esteem, intrinsic motivation, and helping behavior. Furthermore, workload overload has been associated with increased levels of job stress, emotional exhaustion, burnout, and turnover intentions among employees (Barriga Medina et al., 2021; Hong et al., 2023).

Indeed, despite the growing recognition of workload overload as a major concern in today's workplace, several research gaps remain that require further investigation to achieve a comprehensive understanding of workload overload. First, although numerous previous studies have examined the consequences of workload overload on various aspects of employee outcomes, as described above, relatively little attention has been paid to its impact on cybersecurity behavior (Kim et al., 2024; Hong et al., 2023). Investigating the impact of workload overload on cybersecurity behavior is of critical importance in the modern digital landscape. As organizations become increasingly dependent on technology and digital systems, cybersecurity has emerged as a major concern, and the consequences of security breaches and cyberattacks are becoming more severe and widespread (Cascio and Montealegre, 2016). This is a significant gap, as human error and negligence have consistently been identified as the leading causes of cybersecurity incidents (Hadlington et al., 2019). When employees are under the pressure of workload overload, they may be more prone to making errors, taking shortcuts, or engaging in risky behaviors that can leave the organization vulnerable to cyberthreats. For example, a busy employee may be more likely to inadvertently click on a suspicious link in a phishing email, use weak passwords, or fail to properly follow security protocols. Similarly, examining the relationship between workload overload and cybersecurity behavior is crucial for understanding how human factors influence an organization's cybersecurity posture and for developing targeted interventions that can help mitigate the negative effects of high workload on cybersecurity behavior (Efindo, 2012).

Second, the underlying processes (mediators) and conditional factors (moderators) in the relationship between philosophical mindset, workload overload, and cybersecurity behavior have not been extensively investigated. Although two recent papers have demonstrated the mediating role of job stress and organizational identity as well as the moderating role of organizational ethics (Kim et al., 2024), the psychological mechanisms and boundary conditions that shape this relationship have remained largely unexplored. Examining mediators and moderators in a comprehensive manner is essential to develop a more detailed understanding of how philosophical mindset and workload overload affect cybersecurity behavior and when potential interventions can mitigate its negative effects. Specifically, there is a need to examine the role of employees' perception of a deep gap in their relationship with the organization and their experience of a unique state of mental and emotional exhaustion that can ultimately compromise their ability to maintain strong cybersecurity behavior. Furthermore, this paper emphasizes the moderating role of employees' self-efficacy in learning AI in explaining the negative effect of workload overload. The present study addresses this gap by introducing two new ordinal mediators and a new moderator, providing a

deeper and more nuanced understanding of the relationship between philosophical mindset and workload overload and cybersecurity behavior.

A third research gap concerns the less explored moderating factors that can mitigate the negative effects of workload overload in the context of emerging technologies such as AI. The role of AI-related variables, such as self-efficacy in learning AI, has been largely overlooked in the context of workload overload and cybersecurity behavior. As AI continues to change the nature of work (Kaplan and Hanlin, 2019), it is crucial to understand how employees' beliefs about their ability to learn and use AI tools may influence their responses to workload overload and their engagement in cybersecurity practices. Given the increasing importance of AI in the modern workplace, examining how employees' confidence in their ability to learn and use AI technologies can mitigate the negative effects of workload overload makes a significant contribution to the literature. By examining the moderating effect of self-efficacy on AI learning, this study aims to shed light on the potential protective role of AI-related competencies in mitigating the negative impact of workload overload on cybersecurity behavior.

To address the identified research gaps, this study aimed to examine the impact of philosophical mindset and workload overload on employees' cybersecurity behavior, examine the sequential mediating roles of psychological contract breach and burnout, and examine the moderating effect of self-efficacy on AI learning. Psychological contract breach, the first mediator in this study, refers to an employee's perception that his or her employer has failed to fulfill promised commitments, both implicit and explicit, in the employee-organization exchange relationship. This construct goes beyond mere job stress and depicts a deep sense of betrayal and erosion of trust in the employment relationship. When employees experience high workloads, they are more likely to feel that their organization has failed to deliver on its commitments, leading to frustration and disengagement (Kim et al., 2024). This new mediator illuminates the critical role of employee perceptions and expectations in shaping the outcomes of workload overload. The second mediator, burnout, is conceptualized as a state of profound mental and emotional exhaustion that goes beyond job stress or diminished organizational identity. It encompasses a unique combination of fatigue, pessimism, and reduced professional effectiveness resulting from the cumulative effect of high workloads and the violation of mutual obligations between the employee and the organization. When employees experience this state of burnout, they may become highly disengaged from their work, cognitively impaired, and more prone to making mistakes or taking shortcuts in their work, including in the area of cybersecurity. The inclusion of these sequential mediators distinguishes this study from previous research that has focused primarily on job stress and organizational identity as mediators of the relationship between workload overload and cybersecurity behavior (Hong et al., 2023). By proposing and testing a sequential mediation model that incorporates these novel constructs, this study provides a more comprehensive understanding of the psychological processes associated with workload overload and cybersecurity behavior.

Self-efficacy in learning AI refers to an individual's belief in their ability to successfully learn and apply AI concepts, techniques, and tools (Bandura, 1997). This can affect motivation, persistence, and performance in acquiring AI knowledge and skills (Zimmerman, 2000). The aim of this research is to help increase knowledge about the antecedents and consequences of cybersecurity behavior in organizations while providing valuable insights for professionals seeking to promote secure computing practices in the face of increasing work demands and technological advances.

The present study makes a significant contribution to the literature on workload overload, cybersecurity behavior, and the role of AI-related competencies in organizations. First, this research addresses a key gap in our understanding of the factors that influence secure computing practices by examining the impact of philosophical mindset and workload overload on employees' cybersecurity behavior. While previous studies have examined the effects of workload overload on various aspects of employee well-being and performance (e.g., Bolling et al., 2015), the specific relationship between workload overload and cybersecurity behavior has received little attention. Given the increasing importance of cybersecurity in the digital age (Casio and Montealegre, 2016), this study provides valuable insights into how high workloads affect employees' ability to engage in secure computing practices, thereby helping to develop

more effective organizational cybersecurity strategies. Second, this study advances our theoretical understanding of the mechanisms linking philosophical mindset and workload to cybersecurity behavior by examining the mediating roles of psychological contract breach and burnout. By examining these mediating variables, this research provides a more detailed and comprehensive explanation of how philosophical mindset and workload lead to cybersecurity behavior. Examining psychological contract breach as a mediator highlights the importance of the employee-employer relationship in shaping cybersecurity behavior, while examining burnout as a mediator illuminates the role of emotional exhaustion and disengagement in influencing secure computing practices. By identifying these mediating mechanisms, this study helps develop targeted interventions designed to reduce the negative impact of workload on cybersecurity behavior.

Third, this research breaks new ground by examining the role of self-efficacy in AI learning. As AI technologies continue to transform the nature of work (Kaplan & Hanlin, 2019), it is increasingly important to understand how employees' beliefs about their ability to learn and use AI tools may influence their responses to work demands and their engagement in cybersecurity practices. By examining the effect of self-efficacy on AI learning, this study contributes to the growing body of knowledge about the role of AI-related competencies in shaping employee outcomes and provides valuable insights for organizations seeking to promote secure computing practices in the face of technological advances. Finally, this study has significant practical implications for organizations seeking to improve their cybersecurity posture. By identifying workload overload as a potential barrier to employee cybersecurity behavior and highlighting the protective role of self-efficacy on AI learning, this research provides practical insights for managers and HR professionals. Organizations can use these findings to design and implement targeted interventions, such as workload management strategies and AI training programs, to support employees in engaging in secure computing practices. Furthermore, by raising awareness of the mediating roles of psychological contract breach and burnout, this study emphasizes the importance of creating a supportive work environment and addressing employee well-being to promote cybersecurity behavior. Overall, the practical implications of this research can help organizations develop more effective cybersecurity strategies that take into account the complex interplay between job demands, employee competencies, and psychological factors.

Theoretical foundations and research background

Various theoretical frameworks such as the job demand-resource model, resource conservation theory, conservation motivation theory, and effort-reward imbalance model can provide a theoretical framework for understanding the impact of overwork on employees' cybersecurity behavior. According to the job demand-resource model, overwork is a job demand that requires continuous physical, cognitive, and emotional effort, leading to increased strain and possible depletion of personal resources (Baker & Demrotti, 2007). When employees face high levels of overwork, they may experience reduced mental capacity, increased stress, and a reduced ability to focus on tasks that are not directly related to their core job responsibilities. This is consistent with resource conservation theory, which suggests that individuals strive to protect and conserve their limited resources, especially when faced with resource-draining demands such as overwork (Pham et al., 2015). Furthermore, protection motivation theory suggests that individuals' engagement in protective behaviors, such as cybersecurity practices, is influenced by their threat appraisals and coping. However, when cognitive resources are depleted due to high workload, individuals may be less likely to engage in full threat appraisals and coping, leading to reduced cybersecurity behavior. When employees experience high workload, they may be less likely to devote the necessary cognitive resources to cybersecurity tasks because they prioritize their core work responsibilities (Lee et al., 2019). This can lead to reduced cybersecurity behaviors, such as neglecting to update software, using weak passwords, or failing to report suspicious cyber activity. Furthermore, the effort-reward imbalance model further supports this notion, as it posits that when job demands (e.g., high workload) are high and rewards (e.g., time and resources for cybersecurity tasks) are low, employees may become stressed and less likely to engage in discretionary behaviors (Pham et al., 2015). Finally, the interactional theory of stress and coping provides another theoretical perspective through which to

understand the impact of overwork on cybersecurity behavior. According to the interactional theory of stress and coping, when individuals are faced with stressors such as overwork, they engage in a cognitive appraisal process to determine the importance of the stressor and their ability to cope with it. If the stressor is perceived as threatening and the individual's coping resources are perceived as inadequate, they may become stressed and engage in maladaptive coping behaviors. In the field of cybersecurity, overwork may cause employees to perceive cybersecurity tasks as an additional stressor, leading to maladaptive coping behaviors such as ignoring or bypassing cybersecurity policies and practices (Darcy et al., 2014).

Logical thinking is the foundation of employee and manager performance, and an employee must use logical thinking to identify problems and identify appropriate solutions and have logical thinking characteristics. Therefore, an educated, informed, and logically thinking employee is one who is able to resist immediate pressures, avoids hasty decision-making, and emotional behaviors, and who organizes available information with intelligence, patience, and flexibility, and deals with problems logically, and does not get caught up in the mass of information gathering. It is obvious that the management of the organization with such traits in increasing the effectiveness and efficiency of performance, programs and multilateral communications, between individuals and the entire organization, and reflection, accuracy and order of information, stabilizes attention to basic principles in its thinking and takes it into account. The prerequisite for being a successful employee is to have a philosophical mindset. In general, a person with a philosophical mindset tests all his actions, behavior and judgments with the signs of a philosophical mindset. Philosophical mindset is one of the human characteristics that can help employees when facing numerous educational leadership issues and affect cybersecurity behavior (Mohajiran et al., 2014).

Empirical evidence supports the negative relationship between workload overload and cybersecurity behavior. A study by Kim et al. (2024) showed that high workload is negatively related to employees' behaviors to comply with organizational cybersecurity policies. Similarly, a study by Hong et al. (2023) found that high levels of workload lead to reduced cybersecurity behavior. These findings are consistent with the job demand-resource model, resource conservation theory, and protection motivation theory, as high workload depletes employees' cognitive resources and leads to reduced engagement in resource-intensive cybersecurity behaviors (Kim & Kim, 2024).

It is argued that workload overload increases employees' psychological contract violations. Psychological contract violations occur when an employee feels that their organization has failed to fulfill one or more commitments or promises, whether implicit or explicit, that are part of the exchange relationship between the employee and the organization. The psychological contract is a key aspect of the employee-employer relationship, and its violation can lead to negative consequences. Research has shown that psychological contract violations are associated with a range of negative outcomes, including reduced job satisfaction, organizational commitment, and job performance, as well as increased turnover (Zhao et al., 2007).

The job demand-resource model provides a theoretical framework for understanding how workload overload plays a role in psychological contract violations. According to the job demand-resource model, workload overload is a job demand that requires continuous physical, cognitive, and emotional effort, leading to increased strain and possible depletion of personal resources. When employees experience high levels of workload overload, they may perceive that their organization has failed to provide sufficient resources or support to meet their demands, leading to feelings of psychological contract violation (Ball et al., 2008). Resource conservation theory also further supports the link between workload overload and psychological contract violation. Resource conservation theory posits that individuals strive to obtain, maintain, and protect their resources, and stress occurs when these resources are threatened or lost. In the context of workload overload, employees may perceive that their organization has failed to provide sufficient resources to cope with their demands, leading to feelings of resource depletion and psychological contract violation (Kim & Kim, 2024). It is also argued that psychological contract violation increases employees' sense of organizational identity. Burnout is a psychological syndrome characterized by emotional exhaustion, depersonalization, and decreased personal achievement that can occur among people who work with people in some fields. According to Maslach et al. (2001), burnout is a long-term response to chronic emotional and interpersonal stressors in the workplace and is often associated with

human service, education, and health care professionals. The three key dimensions of burnout are: (1) emotional exhaustion, which refers to feelings of over-emotional exhaustion and emptiness; (2) depersonalization, which involves responding negatively, callously, or excessively indifferently to others; and (3) reduced personal achievement, characterized by a reduced sense of competence and productivity at work (Lobade, 2020). Burnout is recognized as a significant occupational health problem with negative consequences for individuals and organizations. For example, a meta-analysis by Alarcon (2011) found that burnout is associated with increased depression, anxiety, and physical health problems, as well as reduced job satisfaction and organizational commitment.

Social exchange theory posits that social relationships involve a set of reciprocal exchanges in which individuals engage with the expectation that their contributions will be reciprocated. In the context of the employee-employer relationship, psychological contracts represent the beliefs that employees have about the reciprocal obligations between themselves and their organizations. When employees perceive that their organization has failed to fulfill its obligations or promises (i.e., a breach of the psychological contract), they may experience feelings of inequality and imbalance in the exchange relationship (Morrison and Robinson, 1997).

In addition, resource conservation theory further supports the link between psychological contract violation and burnout. Resource conservation theory suggests that individuals strive to obtain, maintain, and protect their resources, and stress occurs when these resources are threatened or lost. Psychological contract violation can be viewed as a stressor that depletes employees' resources, as they may invest more time and effort in trying to restore balance to the exchange relationship. This depletion of resources can contribute to burnout, as employees may experience emotional exhaustion, depersonalization, and decreased personal achievement (Kim & Kim, 2024). On the other hand, artificial intelligence is increasingly prevalent in modern organizations, offering benefits such as task automation, improved decision-making, and increased productivity. However, the successful implementation and use of AI systems is highly dependent on employees' self-efficacy in learning AI, which refers to an individual's belief in their ability to learn and effectively apply AI concepts, techniques, and tools (Kim et al., 2024).

The impact of employees' self-efficacy in learning AI on the relationship between workload overload and psychological contract violation can be explained through social cognitive theory and the job demand-resource model. Social cognitive theory suggests that self-efficacy beliefs shape an individual's cognitive, motivational, and emotional processes (Bandura, 1986). Employees who are high in self-efficacy in learning AI are more likely to view workload overload challenges as manageable and to actively seek resources and support to cope with increased demands. They may perceive AI technologies as growth opportunities rather than threats to their psychological contract (Baker & Demrotti, 2017). The job demand-resource model assumes that job resources (e.g., self-efficacy in learning AI) can mitigate the impact of job demands (e.g., workload overload) on stress. Employees who have high self-efficacy in learning AI are more confident in their ability to acquire and effectively apply AI knowledge and skills. When faced with high workloads, they tend to view demands as challenges to be overcome, rather than threats (Ventura et al., 2015). They engage in effective problem-solving strategies and seek resources to cope with increased workloads. As a result, they may feel less violated in their psychological contract because they feel more capable of meeting the demands placed on them (Ng and Lucianti, 2016). For example, in an organization implementing AI-based systems, an employee with high self-efficacy in learning AI who is given additional tasks related to new technology may feel confident in their ability to learn and apply the necessary AI skills. They actively seek out training resources, collaborate with colleagues to develop solutions, and view challenges as opportunities for growth. As a result, they are less likely to feel a breach in their psychological contract. On the other hand, employees with low self-efficacy in learning AI may doubt their ability to acquire and effectively apply AI knowledge and skills. When faced with a high workload, especially in tasks involving AI, they may see the demands as threats rather than challenges. They are more likely to feel overwhelmed and unable to cope with the increased workload, which leads to a higher likelihood of violating their psychological contract (Ng & Lucianti, 2016). Low self-efficacy in learning AI may also prevent employees from seeking resources and support to manage demands. For example, in the same organization

implementing AI-based systems, an employee with low self-efficacy in learning AI who is assigned similar additional tasks may feel overwhelmed and doubt their ability to learn and apply the necessary AI skills. They may struggle to find resources or hesitate to seek support, viewing the increased workload as an insurmountable challenge. As a result, they are more likely to perceive a violation of their psychological contract and feel that the organization has failed to provide sufficient support or resources to help them cope with the demands (Kim & Kim, 2024).

In a study titled The Effect of Workload on Cybersecurity Behavior: A Moderated Mediation Model of Psychological Contract Violation, Burnout, and Self-Efficacy in AI Learning such as ChatGPT, Kim and Kim (2024) examined the effect of overtime on employees' cybersecurity behavior and examined the sequential mediating effects of psychological contract violation and burnout as well as the moderating role of self-efficacy in AI learning. Using the job demand-resource model, resource conservation theory, and social cognition theory, they proposed a moderated mediation model to elucidate the complex relationships among these variables. To test their hypotheses, they conducted a three-wave survey study involving 363 employees from different departments in South Korea. Data were collected using an internet-based survey platform, and the study used stratified random sampling to reduce sampling bias. The results of the structural equation modeling (SEM) analysis showed that overwork indirectly affects cybersecurity behavior through the sequential mediation of psychological contract violation and burnout. In addition, it was found that self-efficacy in learning AI, such as ChatGPT, moderated the relationship between workload overload and psychological contract violation and acted as a buffer to reduce the negative effects of workload overload.

In a study titled Investigating the Impact of Workload Overload on Cybersecurity Behavior: Highlighting Self-efficacy in the Field of AI, Kim et al. (2024) examined the relationship between workload overload and employees' cybersecurity behavior, with a particular focus on the moderating role of self-efficacy in the use of AI. Built within a multidisciplinary theoretical framework, this study integrates concepts from the job demand-resource model, cognitive load theory, social identity theory, and protection motivation theory. Data were collected from 410 employees in South Korea through a three-wave time-lapse survey and analyzed the effect of workload overload on cybersecurity behavior, mediated by job stress and organizational identity, and moderated by self-efficacy in AI. The present study demonstrates the negative effect of workload overload on employees' cybersecurity behavior, mediated by job stress and organizational identity. Also, self-efficacy in using AI significantly moderates the relationship between workload overload and job stress, and reduces the adverse effects of workload on cybersecurity behavior. The findings extend the existing literature by demonstrating how organizational psychology theories can be applied to understand cybersecurity behavior in the workplace. This study emphasizes the importance of managing workload overload and increasing AI self-efficacy to improve cybersecurity practices in organizations.

Hong et al. (2023) in their study titled Reducing the Impact of Workload Overload on Cybersecurity Behavior: The Moderating Effect of Organizational Ethics - A Mediated Moderation Analysis examined how workload affects cybersecurity behavior, using job stress as a mediator and organizational ethics as a moderator. Using a time-lagged survey design, 377 South Korean employees were surveyed. The results of SEM (Structural Equation Modeling) analysis indicate that high workload leads to higher job stress, which in turn worsens cybersecurity behavior. High levels of organizational ethics moderate this negative relationship.

Alizadeh Soodmand et al. (1403) conducted a study to explain the relationship and effectiveness of cyber security and defense components in information-based organizations in the country. The research population is managers, experts, security officials, etc. of organizations. The sample size obtained was 157, only 88 of these organizations agreed to participate in the research. Interviews with experts, library resources, articles, and questionnaire tools were used to collect data and to measure validity, face-content validity and Cronbach's alpha coefficient were used for reliability, and SPSS (25) software was used to analyze data and test hypotheses. In the descriptive statistics section, dispersion indices were used, and in the inferential statistics section, Kolmogorov-Smirnov tests were used to assess the normality of the data,

and Pearson's correlation coefficient was used to examine the relationship between variables. Analysis of the research data showed that there is a significant relationship between the factors and components of the research; also, there is an acceptable correlation between the variables; There is a security policy, organizational security, etc. The relationship between the variables and effective scales of the research has been measured. The results obtained in the first part showed that the components of security and cyber defense; security policy, asset classification and management, etc. have a significant relationship and have a direct impact on the overall performance of information-oriented organizations. Further examination of the results revealed that the relationship between components such as employee security, physical security and scales such as year of organization, annual transaction, etc. has a direct impact on improving the security and cyber defense of these organizations; it was also found that there is no relationship between variables such as the number of security staff and security policy, and the relationship between security staff variables and system maintenance and support is in the opposite direction; therefore, this reduces the productivity of security staff in information-oriented organizations.

Jahdi et al. (1402) studied the effect of organizational factors related to work, protection motivation, and planned behavior on protecting information security in the Islamic Republic of Iran Shipping Organization. The statistical population of this study is all employees of the Islamic Republic of Iran Shipping Organization in the information technology department, which is about 1500 people. Also, the sample size was calculated according to the Cochran formula to be 320 people, who were sampled non-probably. Structural equation modeling and SmartPLS software were used to analyze the data. The results of the study showed that the variables of organizational commitment, job satisfaction, threat sensitivity, threat severity, self-efficacy, accountability cost, attitude, perceived behavioral control, and subjective norms have a significant effect on the motivation to protect information. Also, the significant effect of the motivation to protect information security on information security protective behaviors was also confirmed.

Research hypotheses

In order to achieve the research objectives and theoretical foundations, the following hypotheses were designed for the study:

-1Workload has a significant effect on cybersecurity behavior.

-2Workload has a significant effect on psychological contract violation behavior.

-3Workload has a significant effect on job burnout.

-4Workload has a significant effect on self-efficacy in interaction with artificial intelligence.

-5Philosophical mindset has a significant effect on cybersecurity behavior.

-6Philosophical mindset has a significant effect on psychological contract violation behavior.

-7Philosophical mindset has a significant effect on job burnout.

-8Philosophical mindset has a significant effect on self-efficacy in interaction with artificial intelligence.

-9Psychological contract violation has a significant effect on cybersecurity behavior.

-10Job burnout has a significant effect on cybersecurity behavior.

-11Self-efficacy in interaction with artificial intelligence has a significant effect on cybersecurity behavior.

Based on the theoretical foundations and research hypotheses, the conceptual model of the research was designed as shown in Figure.(1)

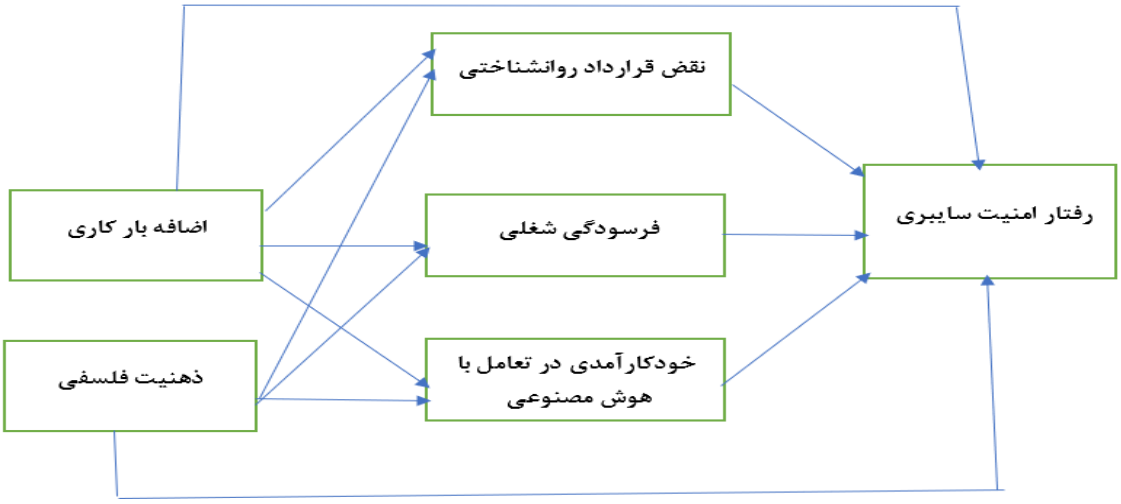

Figure 1: Conceptual model of the research

Research methodology

The method of this research is of an applied type from the perspective of explaining the purpose; and from the perspective of collecting data, it is a descriptive survey type conducted by a questionnaire. Implementing descriptive research can be for better understanding the current situation or assisting in the decision-making process.

In this research, two methods are used to collect information:

.1Library study: The method related to the literature and theoretical foundations is the library method.

.2Field study: The method related to collecting information on variables is a questionnaire and a survey.

The statistical population of the research was managers and employees of knowledge-based companies in Iran, and based on the Morgan table, a sample size of 384 people was considered. For greater certainty, 400 questionnaires were distributed among the target population, of which 391 questionnaires were capable of analysis. A standard questionnaire was used in this research. The questionnaire of this research consists of three parts.

Research findings

In this study, the partial least squares (PLS) method was used, which consists of two main stages: 1) examining the fit of the measurement models, the structural model, and the general model, and 2) testing the relationships between the constructs.

Examining the fit of the measurement models

In the partial least squares (PLS) method, the following items are examined for the evaluation of the questionnaire and confirmatory factor analysis: Cronbach's alpha; composite reliability (CR); factor loading coefficients and their significance; examining the validity of the average variance extracted (AVE); Fornell and Larker matrix.

Table 1: Factor loading values and their significance, Cronbach's alpha, composite reliability, average variance extracted (AVE)

AVE	CR	Cronbach's alpha	T-coefficient	Factor loading	Items	Variables
0.627	0.893	0.851	۸۰.۰۲۶	۰.۸۶0	EB1	Workload
			۳۷.۱۳۹	۰.۷۹۶	EB2	

AVE	CR	Cronbach's alpha	T-coefficient	Factor loading	Items	Variables
			۲۶.۷۶0	۰.۷۲۸	EB3	
			۲۸.۴۹۵	۰.۷۳۶	EB4	
			۴۷.۳۵۹	۰.۸۳۲	EB5	
0.665	0.856	0.748	۳۹.۷۲۱	۰.۸00	ZF1	Philosophical mindset
			۴۱.۷۹۹	۰.۸۰۹	ZF2	
			۵۰.۷۲۲	۰.۸۳۸	ZF3	
0.584	0.875	0.822	۳۲.۴۸۱	۰.۷۶۵	NG1	Psychological contract breach
			۴۳.۷۲۶	۰.۷۹۶	NG2	
			۲۴.۱۹0	۰.۷۱۸	NG3	
			۲۶.۱۷۳	۰.۷۵۹	NG4	
			۳۷.۱۷۳	۰.۷۸۱	NG5	
0.554	0.897	0.866	۲۴.۷۶۲	۰.۷۳۳	FS1	Burnout
			۲۵.۵۱۵	۰.۷۱۸	FS2	
			۳۷.۴۸۲	۰.۷۷۵	FS3	
			۲۸.۶۲۹	۰.۷۴۲	FS4	
			۳۱.۳۰۵	۰.۷۵۷	FS5	
			۲۷.۱۷۲	۰.۷۱۷	FS6	
			34.000	۰.۷۶۸	FS7	
0.608	0.886	0.838	۴۲.۹۵۸	۰.۸۱۹	KA1	Self-efficacy in learning AI
			۲۹.۹۹۳	۰.۷۸۵	KA2	
			۲۶.۹۵0	۰.۷۴۸	KA3	
			۳۰.۷۹۷	۰.۷۶۸	KA4	
			۳۱.۴۶۷	۰.۷۷۷	KA5	
0.614	0.888	0.843	۴۲.۴۹۷	۰.۸۰۳	RA1	Cybersecurity behavior
			۳۱.۸۷۸	۰.۷۵۳	RA2	
			۳۳.۳۹0	۰.۷۶۹	RA3	
			۴۰.۵۰۱	۰.۸۱0	RA4	
			۳۵.۸۲۱	۰.۷۸۲	RA5	

The factor loading of all measures is more than 0.5; Cronbach's alpha coefficient and composite reliability of all variables are more than 0.7 and the average variance extracted (AVE) of all variables is more than 0.5 and is reported to be acceptable.

The divergent validity examination in PLS is carried out by means of a matrix whose cells contain the correlation coefficients between the constructs and the square root of the AVE values related to each construct. The research model has acceptable divergent validity if the numbers in the main diagonal of the matrix are greater than their lower values. Table 2 shows this matrix. As can be seen, the divergent validity of the model is acceptable.

Table 2: Divergent validity (Fornell and Larker method)

Variables	Workload overload	Self-efficacy in learning artificial intelligence	Philosophical mindset	Cybersecurity Behavior	Job burnout	Breach of psychological contract
Workload	۰.۷۹۲					
Self-efficacy in learning AI	-۰.۸۴۵	۰.۷۸0				
Philosophical mindset	-۰.۸۱۶	۰.۷۰۶	۰.۸۱۶			
Cybersecurity behavior	-۰.۸۴0	۰.۷۰۷	۰.۷۰۸	۰.۷۸۴		
Burnout	۰.۷۳۱	-۰.۸۳۲	-۰.۸۱۹	-۰.۸۳۱	۰.۷۴۴	

Breach of psychological contract	۰.۷۵۷	-۰.۸۳۶	-۰.۷۹۴	-۰.۸۲۱	۰.۷۳۷	۰.۷۶۴

Structural Model Fit Examination

The most basic criterion for measuring the relationship between the constructs in the model (structural section) is the t-significance numbers. If the value of these numbers exceeds 1.96, it indicates the accuracy of the relationship between the constructs and, as a result, the research hypotheses are confirmed. Of course, t-numbers only indicate the accuracy of the relationships and cannot measure the intensity of the relationship between the constructs. As can be seen in Figures 2 and 3, the structural model is presented in two modes: coefficient estimation and path coefficient significance. Table 3 shows the t-significance coefficients for the relationships between the research constructs.

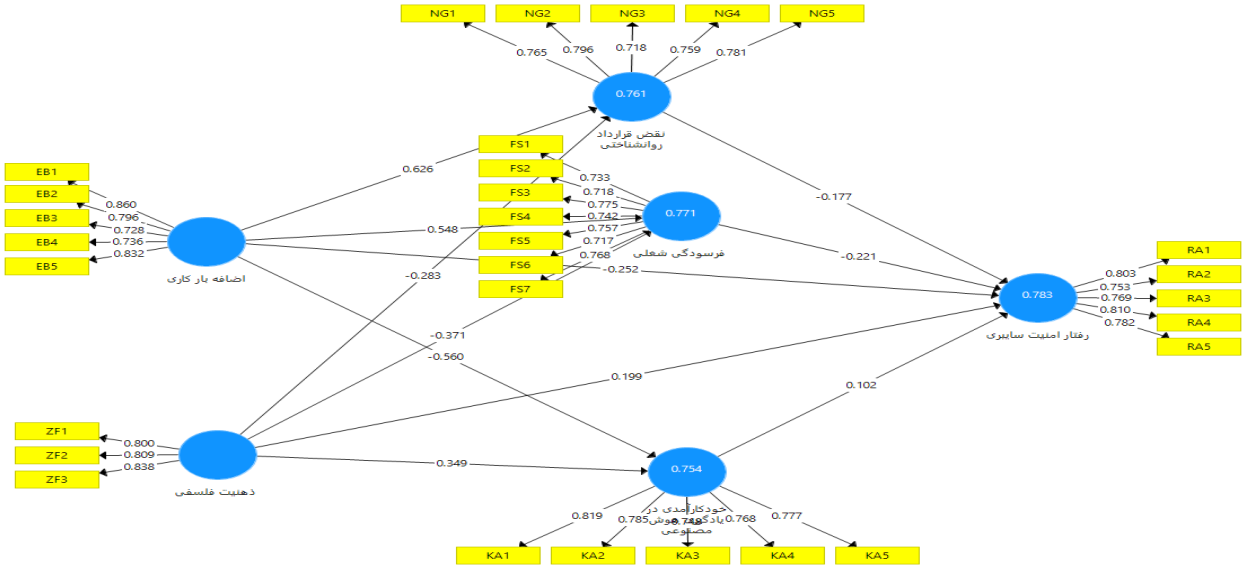

Figure 2: Structural model in the case of estimating standard coefficients

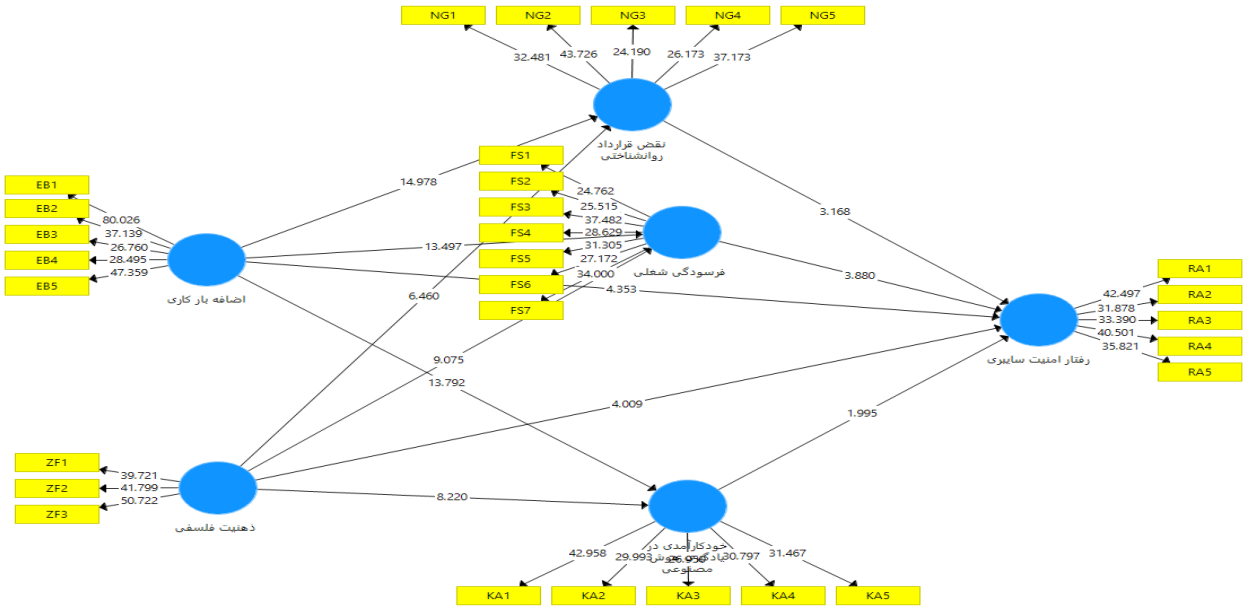

Figure 3: Structural model in the case of coefficient significance (t.value)

Table 3: Path coefficients and t-significance coefficients for relationships between research constructs

Result	t-value	Path coefficients	The path of the relationship between hidden structures	
It makes sense	4.353	-0.252	RA ← EB	1
It makes sense	14.978	0.626	NG ← EB	2
It makes sense	13.497	0.548	FS ← EB	3
It makes sense	13.792	-0.560	KA ← EB	4
It makes sense	4.009	0.199	RA ← ZF	5
It makes sense	6.460	-0.283	NG ← ZF	6
It makes sense	9.075	-0.371	FS ← ZF	7
It makes sense	8.220	0.349	KA ← ZF	8
It makes sense	3.168	-0.177	RA ← NG	9
It makes sense	3.880	-0.221	RA ← FS	10
It makes sense	1.995	0.102	RA ← KA	11

Coefficient of Determination (R2) Criteria for Endogenous Latent Variables

Researchers have introduced three values of 0.19, 0.33, and 0.67 as criteria for weak, medium, and strong R2 values. The R2 values for the endogenous latent variables of the model are presented in Table 4. As can be seen, the model variables have appropriate coefficient of determination values.

Table 4: R2 values for endogenous variables of the model

R2	Variables
۰.۷۵۴	Self-efficacy in learning AI
۰.۷۸۳	Cybersecurity behavior
۰.۷۷۱	Burnout
۰.۷۶۱	Breach of psychological contract

Effect size criterion) f^2(

To determine the strength of the relationship between the latent variables in the model, the researchers introduced the effect size criterion. The values 0.02, 0.15, and 0.35 indicate the small, medium, and large effect sizes of one construct on another, respectively.

Table 5: Effect size coefficients f^2

f^2	Affective (dependent) variable	Influential Variable (Independent)
0.426	Self-efficacy in learning AI	Workload
0.052	Cybersecurity behavior	
0.438	Burnout	
0.549	Breach of psychological contract	
0.010	Cybersecurity Behavior	Self-efficacy in Learning Artificial Intelligence
0.166	Self-Efficacy in Learning Artificial Intelligence	Philosophical Mindset
0.047	Cybersecurity Behavior	
0.201	Burnout	

0.112	Breach of Psychological Contract	
0.045	Cybersecurity Behavior	Burnout
0.029		Breach of the Psychological Contract

Model predictive power criterion (Q2)

The researchers have determined three values of 0.02, 0.15 and 0.35 for this criterion, which respectively indicate the weak, moderate and strong predictive power of the model regarding the endogenous construct indicators. Table 6 shows the Q2 values related to the endogenous constructs of the model, which indicate an acceptable fit of the structural model.

Table 6: Q2 values related to the endogenous variables of the model

Q2	Variables
0.454	Self-efficacy in learning AI
0.475	Cybersecurity behavior
0.422	Burnout
0.440	Breach of psychological contract

Checking the overall model fit

The GOF criterion is used to check the overall model fit, which controls both the measurement and structural model parts.

Table 7: Average Communicability Values and Average R Squares Values

$\overline{R^2}$	$\overline{Communalities}$
0.767	0.608
$GOF = \sqrt{0.767 \times 0.608} = 0.682$	
Three values of 0.01, 0.25, and 0.36 represent weak, moderate, and strong fit, respectively.	

The GOF value is 0.682, indicating an acceptable fit.

Hypothesis Testing

To confirm the hypotheses, the t value must be equal to or greater than 1.96. Otherwise, the hypothesis is rejected. In this study, 11 hypotheses were tested, the results of which are given in Table 8.

Table 8: Hypotheses and Summary of Research Results

Result	T-value	Path coefficient (B)	Hypotheses	Row
Confirm	4.353	-0.252	Overload has a significant effect on cybersecurity behavior.	1
Confirm	14.978	0.626	Overload has a significant effect on psychological contract violation behavior.	2
Confirm	13.497	0.548	Overload has a significant effect on burnout.	3
Confirm	13.792	-0.560	Overload has a significant effect on self-efficacy in interacting with artificial intelligence.	4
Confirm	4.009	0.199	Philosophical mindset has a significant effect on cybersecurity behavior.	5

Confirm	6.460	-0.283	Philosophical mindset has a significant effect on psychological contract violation behavior.	6
Confirm	9.075	-0.371	Philosophical mindset has a significant effect on burnout.	7
Confirm	8.220	0.349	Philosophical mindset has a significant effect on self-efficacy in interacting with artificial intelligence.	8
Confirm	3.168	-0.177	Psychological contract violation has a significant effect on cybersecurity behavior.	9
Confirm	3.880	-0.221	Burnout has a significant effect on cybersecurity behavior.	10
Confirm	1.995	0.102	Self-efficacy in interacting with artificial intelligence has a significant effect on cybersecurity behavior.	11

The results of the path analysis show that all research hypotheses are accepted.

Results and Discussion

The results of the present study show that workload overload, as an organizational stressor, has multifaceted and mainly negative effects on employee behaviors and psychological states. On the one hand, workload overload is associated with a decrease in cybersecurity behavior and self-efficacy in interacting with artificial intelligence, which is likely due to the depletion of cognitive and emotional resources of employees under work pressure. This finding is consistent with studies such as Kim and Kim (2024) that show that high workload reduces employees' focus on security protocols. On the other hand, workload overload leads to increased psychological contract violations and burnout, which is consistent with the research of Maslech and Leiter (2023); they emphasize that unreasonable workload reinforces feelings of injustice and lack of commitment in employees. Philosophical mindset, as a positive moderating variable, reduces the detrimental effects of workload overload. This mindset improves cybersecurity behavior and self-efficacy in interacting with AI by enhancing critical thinking and flexibility, while simultaneously increasing employee resilience by reducing psychological contract violation and burnout. Philosophical thinking enhances the ability to solve complex problems and manage ethical conflicts. Also, the role of self-efficacy in interacting with AI as a reinforcing factor of security behaviors is consistent with the emphasis on the importance of individual beliefs in implementing responsible behaviors. On the other hand, psychological contract violation and burnout as key mediators show an inverse relationship with cybersecurity behavior. These findings are consistent with cybersecurity stress-models such as Kim and Kim (2024) that consider organizational stress as a factor in reducing attention to security protocols. In contrast, self-efficacy in interacting with AI as a facilitating mechanism not only improves security behaviors but also reduces the gap between technology and users. Overall, this research confirms that organizational (e.g., workload) and individual (e.g., philosophical mindset) factors interact to influence cybersecurity. These findings support the conservation of resources theory, which emphasizes the role of psychological resources in coping with stress and implementing desirable behaviors.

Practical suggestions for knowledge-based companies

.1Reduce workload:

•Use artificial intelligence to automate repetitive tasks such as data processing and reporting, manage employee workload.

•Implement smart alert systems to identify and redistribute tasks during peak workloads.

•Conduct time management workshops focusing on task prioritization and delegation.

.2Strengthen philosophical mindset and self-efficacy:

•Design critical thinking training courses focused on cybersecurity challenges and technology ethics.

•Use artificial intelligence simulators to provide hands-on training to employees and increase their confidence in dealing with technology.

•Create a space for open questioning in teams so that employees can analyze security issues without fear of judgment.

.3Psychological contract management and burnout:

•Conduct periodic job satisfaction surveys and individual interviews to identify feelings of breach of commitment early.

•Develop mental health programs such as counseling sessions and mindfulness exercises to reduce burnout.

•Design a security performance-based reward system to reinforce responsible cyber behaviors.

Suggestions for future research

.1Extend the model to new areas:

•Examine the impact of organizational culture or transformational leadership style on the relationship between workload overload and cybersecurity behavior.

•Comparative study of this model in the fintech and digital health industries to identify contextual differences.

•Analyze the role of facilitating artificial intelligence (such as smart assistants) in reducing workload and improving self-efficacy.

.2Methodology and theoretical development:

•Conduct longitudinal studies to examine the long-term effects of philosophical mindset on cybersecurity.

•Using mixed methods (qualitative-quantitative) to explore more deeply the psychological mechanisms associated with breach of contract.

•Designing predictive AI tools to identify employees at risk of burnout based on behavioral patterns.

By revealing the complex relationships between work stress, philosophical mindset, and security behaviors, this research provides a valuable framework for knowledge-based companies to improve both productivity and cybersecurity with a holistic approach. Future research could extend the model to new domains to gain a deeper understanding of human-technology interaction.

References

1. Johdi, Ali; Kiakjori, Karim and Hosseini Sayadnourd, Monireh. (2013). The effect of organizational factors related to work, protection motivation and planned behavior on information security protection in the Islamic Republic of Iran Shipping Organization. Maritime Sciences Education, 10(3), 95-108.
2. Hosseini-Sanoo, Amin and Kadkhoda, Negar. (2010). The effectiveness of information systems security, resulting from the effect of institutional theory dimensions on employees' organizational behavior. Scientific Journal of Intelligent Business Management Studies, 8(32), 180-147.
3. Alizadeh Soedmand, Alireza; Fathi Hafeshjani, Kiamarth; Shah Mansouri, Ashraf and Arab Sorkh, Abuzar. (2014). Explaining the relationship and effectiveness of cyber security and defense components in information-oriented organizations of the country. Quarterly Journal of Security and Law Enforcement Studies. 19.(1)
4. Mohajeran, Behnaz; Qaleh, Alireza; Hamzeh Robati, Motaharah; Nami, Kulsoom and Nemati, Abdolrazzaq. (2015). Investigating the relationship between philosophical mindset and entrepreneurial personality traits of school principals. Management and Development Process, 28 (3), 130-107.
5. Alarcon, G. M. (2011). A meta-analysis of burnout with job demands, resources, and attitudes. *Journal of vocational behavior*, *79*(2), 549-562.
6. Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. *Journal of managerial psychology*, *22*(3), 309-328.
7. Bakker, A. B., & Demerouti, E. (2017). Job demands–resources theory: Taking stock and looking forward. *Journal of occupational health psychology*, *22*(3), 273.

8. Bal, P. M., De Lange, A. H., Jansen, P. G., & Van Der Velde, M. E. (2008). Psychological contract breach and job attitudes: A meta-analysis of age as a moderator. *Journal of vocational behavior*, *72*(1), 143-158.
9. Bandura, A. (1986). Social foundations of thought and action. *Englewood Cliffs, NJ*, *1986*(23-28), 2.
10. Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan.
11. Barriga Medina, H. R., Campoverde Aguirre, R., Coello-Montecel, D., Ochoa Pacheco, P., & Paredes-Aguirre, M. I. (2021). The influence of work–family conflict on burnout during the COVID-19 pandemic: The effect of teleworking overload. *International journal of environmental research and public health*, *18*(19), 10302.
12. Bowling, N. A., Alarcon, G. M., Bragg, C. B., & Hartman, M. J. (2015). A meta-analytic examination of the potential correlates and consequences of workload. *Work & stress*, *29*(2), 95-113.
13. Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. *Annual review of organizational psychology and organizational behavior*, *3*(1), 349-375.
14. 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.
15. Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41-48.
16. Hong, Y., Kim, M. J., & Roh, T. (2023). Mitigating the impact of work overload on Cybersecurity Behavior: The moderating influence of corporate Ethics—A mediated moderation analysis. *Sustainability*, *15*(19), 14327.
17. 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.
18. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business horizons*, *62*(1), 15-25.
19. Kim, B. J., & Kim, M. J. (2024). The influence of work overload on cybersecurity behavior: A moderated mediation model of psychological contract breach, burnout, and self-efficacy in AI learning such as ChatGPT. *Technology in Society*, *77*, 102543.
20. Kim, B. J., Kim, M. J., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior: Highlighting self-efficacy in the realm of artificial intelligence. *Current Psychology*, *43*(19), 17146-17162.
21. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International journal of information management*, *45*, 13-24.
22. Lubbadeh, T. (2020). Job burnout: A general literature review. *International Review of Management and Marketing*, *10*(3), 7.
23. Maslach, C., & Leiter, M. P. (2023). The Burnout Challenge: Managing People's Relationships with Their Jobs. TD Magazine, 77(1), 69-70.
24. Maslach, C., Schaufeli., W.B., Leiter, M.P. (2001). Job burnout, Annu. Rev. Psychol. 52, 397–422.
25. Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: A model of how psychological contract violation develops. *Academy of management Review*, *22*(1), 226-256.
26. Ng, T. W., & Lucianetti, L. (2016). Within-individual increases in innovative behavior and creative, persuasion, and change self-efficacy over time: A social–cognitive theory perspective. *Journal of applied psychology*, *101*(1), 14.
27. Pham, C. H., El-Den, J., & Richardson, J. (2015). Influence of security compliance demands and resources on security compliance-an exploratory study in Vietnam.
28. Ventura, M., Salanova, M., & Llorens, S. (2015). Professional self-efficacy as a predictor of burnout and engagement: The role of challenge and hindrance demands. *The Journal of psychology*, *149*(3), 277-302.
29. Zhao, H. A. O., Wayne, S. J., Glibkowski, B. C., & Bravo, J. (2007). The impact of psychological contract breach on work-related outcomes: a meta-analysis. *Personnel psychology*, *60*(3), 647-680.
30. Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. *Contemporary educational psychology*, *25*(1), 82-91.