

Article

Mitigating the Impact of Work Overload on Cybersecurity Behavior: The Moderating Influence of Corporate Ethics—A Mediated Moderation Analysis

Yunsook Hong ¹, Min-Jik Kim ^{2,*} and Taewoo Roh ^{3,*}

¹ College of Business Administration, University of Ulsan, Ulsan 44610, Republic of Korea; yhong@ulsan.ac.kr

² School of Industrial Management, Korea University of Technology and Education, Cheonan 31253, Republic of Korea

³ School of International Studies, Hanyang University, Seoul 04763, Republic of Korea

* Correspondence: mkim@koreatech.ac.kr (M.-J.K.); twroh@hanyang.ac.kr (T.R.)

Abstract: This present study examines how work overload affects cybersecurity behavior, considering job stress as a mediator and corporate ethics as a moderator. Using a time-lagged survey design, 377 South Korean employees were surveyed. The results of SEM analysis (structural equation model) show that work overload leads to higher job stress, which in turn worsens cybersecurity behavior. High levels of corporate ethics buffer this negative relationship. This research fills gaps in the existing literature by linking work overload, job stress, and corporate ethics to cybersecurity behavior, offering valuable insights for both theory and practice. Future research directions are also discussed.

Keywords: work overload; cybersecurity behavior; job stress; corporate ethics; moderated mediation model



Citation: Hong, Y.; Kim, M.-J.; Roh, T. Mitigating the Impact of Work Overload on Cybersecurity Behavior: The Moderating Influence of Corporate Ethics—A Mediated Moderation Analysis. *Sustainability* **2023**, *15*, 14327. <https://doi.org/10.3390/su151914327>

Academic Editor: Harris Wu

Received: 16 August 2023

Revised: 12 September 2023

Accepted: 18 September 2023

Published: 28 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the highly competitive landscape of the contemporary business environment, personnel across a vast array of corporate structures are grappling with substantial workloads. This results in an escalated mental and physical strain on employees, stemming from an accumulation of onerous responsibilities in their professional roles. For example, the COVID-19 pandemic has caused workers across various industries—including healthcare, government, and private businesses—to experience increased workloads [1]. In addition to their normal tasks, workers must take on extra responsibilities to prevent the spread of the coronavirus, leading them to feel overburdened [2]. This is known as work overload, a phenomenon that occurs when individuals feel their jobs demand too much from them in terms of quantity or intensity of responsibilities [3]. Work overload is a widely studied construct within organizational behavior and occupational health psychology. It refers to the perception that the demands of one's job, including the amount of work and excessive time pressures, surpass one's capabilities to perform them effectively [4]. Work overload may arise due to high task complexity, tight deadlines, or extensive working hours that exceed the individual's capacities or resources [5–8].

Research has shown that work overload can have several adverse effects. It can lead to increased job stress, burnout, emotional exhaustion, conflict between work and family life, and turnover intention, and it can lower job satisfaction, self-esteem, intrinsic motivation, organizational identification, and job performance [7–16]. Moreover, it has been associated with negative health outcomes, such as sleep disturbances, cardiovascular problems, and other physical and mental health issues [17–21].

Although numerous studies have explicated the influence of workload overload on diverse outcomes within an organization, research gaps remain in the literature. First, although work overload has been extensively examined in the context of various organizational outcomes such as job satisfaction, work performance, and physical and mental

health [9–11], its influence on employee cybersecurity behavior remains underexplored [22]. Cybersecurity behavior refers to the actions individuals or organizations take to protect their information systems and networks from security incidents, breaches, or attacks [22]. The rapid advancement of digital technologies and the exponential growth in the use of information systems in organizational contexts have substantially heightened the importance of cybersecurity. The increased interconnectivity has made organizations vulnerable to various cyber threats, emphasizing the significance of employee cybersecurity behavior [23–27]. Despite this criticality, there is a paucity of research that comprehensively examines the influence of work overload on cybersecurity behavior, leaving significant gaps in the literature that need to be addressed. Given the paramount importance of safeguarding organizational information assets in this digital era [25–27], the need to investigate the impact of work conditions, specifically work overload, on cybersecurity behavior becomes crucial.

Second, the mechanisms and processes through which work overload influences cybersecurity behavior have not been thoroughly explored in the literature [6–8]. The mediating role of job stress on the relationship between work overload and cybersecurity behavior is not yet understood in depth. Understanding the mediating mechanism is critical because understanding it provides insights into the underlying processes that link work overload and cybersecurity behavior, offering opportunities for practical interventions [28].

Third, the contingent role of organizational-level variables such as corporate ethics has been largely overlooked in the work overload–cybersecurity behavior relationship [6–8]. Corporate ethics is a crucial aspect of the workplace that can potentially buffer the adverse effects of work overload on employee outcomes [29]. Hence, investigating the moderating role of corporate ethics can provide nuanced insights into the conditions under which work overload affects cybersecurity behavior.

In sum, in the digital age, as organizations rapidly integrate technology into their daily operations, the significance of cyber security behavior among employees has come to the fore. This importance is further magnified given the increasing complexities of modern organizational structures, shifting dynamics of work, and the rise in cyber threats. It is within this evolving landscape that our study is situated, aiming to shed light on the underpinnings of cyber security behavior, specifically focusing on the influence of work overload. In light of these gaps, the objectives of this study are threefold:

1. Investigate the relationship between work overload and cyber security behavior among employees.
2. Examine job stress as a mediating variable in this relationship.
3. Explore the moderating effect of organizational ethics on the relationship between work overload and job stress.

The justification for this study lies in its potential to significantly advance our knowledge in a domain of pressing contemporary relevance. By unveiling the nuanced interplay of work overload, job stress, and organizational ethics in determining cyber security behavior, this research provides both theoretical insights for scholars and practical guidance for practitioners aiming to bolster cyber resilience in organizations.

To complement the above issues, this study addresses the research gaps by investigating the influence of work overload on employee cybersecurity behavior, the mediating role of job stress, and the moderating role of corporate ethics.

2. Theory and Hypotheses

2.1. Work Overload and Cybersecurity Behavior

We propose that employee work overload will decrease the degree of their cybersecurity behavior. Work overload is a concept widely discussed within the realm of organizational psychology and job stress research. It refers to a state where the demands of a job exceed the time, resources, or capabilities available to an employee to perform the tasks or responsibilities associated with the job [30–32]. These demands may come in the form of excess hours, too many tasks, or tasks that are too complex [33]. Work overload can be categorized into quantitative overload, where an employee is overwhelmed by the sheer

number of tasks or a lack of time to perform them, and qualitative overload, where the complexity or difficulty of the tasks surpass the employee's capabilities or resources [34].

Cybersecurity behavior means the actions individuals or organizations take to protect their information systems and networks from security incidents, breaches, or attacks [22]. This behavior can be preventive, reactive, or adaptive. Preventive behaviors mitigate risks before an incident occurs, reactive behaviors respond to an incident after it occurs, and adaptive behaviors involve changing practices based on past incidents or new information about potential threats [35]. In the individual context, cybersecurity behavior involves actions such as creating and managing strong passwords, avoiding suspicious emails or websites, regularly updating and patching software, using secure networks, and backing up data [36]. Research has shown that these behaviors are influenced by a range of factors, including individuals' knowledge, attitudes, and perceptions of threat and vulnerability as well as organizational culture, policies, and training [24–27,37].

In the organizational context, cybersecurity behavior involves implementing and managing security measures such as firewalls, intrusion detection systems, and encryption as well as developing and enforcing security policies and procedures, conducting regular audits and risk assessments, and providing employee training [26,27,38]. Organizational cybersecurity behavior is influenced by factors such as leadership commitment, organizational culture, regulatory environment, and resource availability [26,27,39].

Work overload and its implications for cybersecurity behavior constitute a crucial concern within the organizational milieu. This impact is substantiated through multiple theoretical frameworks, each of which furnishes distinct yet complementary perspectives.

The Job Demand–Control model [40] explicates how high job demands (such as work overload) coupled with low job control can breed a stress-inducing work environment. Under such circumstances, employees might inadvertently bypass cybersecurity practices in a bid to manage their workload. This inadvertent neglect towards cybersecurity protocols can potentially heighten the susceptibility to cyber threats, highlighting the criticality of maintaining an optimal workload [41].

The Effort–Reward Imbalance model [42] offers another perspective. Here, an imbalance between effort (manifested as work overload) and reward can precipitate a diminished commitment toward one's job role, which inevitably includes adherence to cybersecurity policies. This underlines the necessity of establishing an equitable effort–reward ratio to ensure optimal cybersecurity behavior [43,44].

Lastly, the Conservation of Resources theory [45,46] elucidates how persistent work overload can exhaust an employee's resources, both mental and physical. As resources are depleted, individuals are prone to focus on immediate, pressing tasks, thereby sidelining longer-term responsibilities such as following cybersecurity policies and procedures. This suggests that managing work overload is critical not just for employees' well-being but also to ensure consistent adherence to cybersecurity practices [47,48].

Together, these theoretical frameworks illuminate the multifaceted impacts of work overload on cybersecurity behavior, underscoring the importance of carefully managing workload to minimize the potential cybersecurity risks.

Hypothesis 1. *Work overload negatively affects employee cybersecurity behavior.*

2.2. Work Overload and Job Stress

Work overload, recognized as a core component of job demands, is posited to be a substantial contributor to job stress [49]. Job stress is known as a chronic condition characterized by physical and emotional responses that occur when the requirements of the job do not match the capabilities, resources, or needs of the worker [30]. Job stress results from the interactions between the worker and the work conditions, and it can lead to poor health and even injury [50]. A variety of factors can contribute to job stress, such as work overload, role conflicts and ambiguity, lack of job control, interpersonal conflicts, organizational culture, and management style [51,52]. Research has found a

strong relationship between job stress and various health outcomes. High levels of job stress are associated with a number of psychological symptoms, such as anxiety, depression, burnout, and decreased job satisfaction, as well as physical health problems, such as cardiovascular disease, musculoskeletal disorders, and impaired immune function [53,54].

To be specific, we propose that increased work overload will increase the degree of employee job stress. This view has its roots in the Job Demand–Control model [40], in which work overload is conceived as a crucial job demand that, due to an imbalance between tasks and available time, instigates psychological strain, hence precipitating job stress.

Karasek’s Job Demand–Control model asserts that the combination of high job demands and low job control leads to strain and potential health problems, both physical and psychological. When work demands such as workload, time pressure, and role conflict exceed the individual’s coping ability, the situation becomes stressful, leading to negative health outcomes. The Job Demand–Control model has been extensively tested and supported in various empirical studies, such as Häusser, Mojzisch, Niesel, and Schulz-Hardt [55], Parker [47], and Pham, Brennan, and Furnell [48].

The Effort–Reward Imbalance model [42] provides another valuable perspective. It posits that employees feel stressed when their effort (i.e., workload) is not met with corresponding rewards (e.g., pay, esteem, or career opportunities including job security). Persistent high efforts (i.e., work overload) combined with few rewards leads to emotional distress and can initiate stress-related diseases [47,48].

Moreover, the Conservation of Resources theory [45,46] suggests that individuals strive to obtain, retain, and protect valuable resources. In this case, work overload can lead to resource (time and energy) depletion, thereby initiating a stress response.

Accordingly, each of these theoretical perspectives provides a solid grounding for the proposition that increased work overload can increase job stress.

Hypothesis 2. *Work overload positively affects employee job stress.*

2.3. Job Stress and Cybersecurity Behavior

The relationship between job stress and cybersecurity behavior is an emergent area of focus within organizational research as businesses grapple with securing their cyber infrastructure [24–27]. Cybersecurity behavior refers to the actions individuals or organizations take to protect their information systems and networks from security incidents, breaches, or attacks [22]. There has been increasing recognition of the critical role of human behavior in cybersecurity, given that many security incidents and breaches result from human error or risky behavior, even in the presence of advanced security technologies [22].

To be specific, we suggest that the increased job stress will decrease the level of employee cybersecurity behavior based on a variety of theoretical background information. First, the General Strain Theory of criminology [56] can be repurposed to explain this relationship. According to the theory, individuals experiencing strain or stress may be more likely to engage in deviant behavior, including non-compliant cybersecurity behaviors. This relationship has been examined in the context of information security, suggesting that job stress can lead to employee neglect or violation of cybersecurity policies [43,44,57]. Also, this theory suggests that when individuals face strain or stress, they are more likely to exhibit deviant behavior as a coping mechanism. In the context of job stress, employees might overlook cybersecurity norms due to their high stress levels, thereby exposing the organization to potential cybersecurity risks [44,58].

The Job Demands–Resources model [58] can be drawn upon to conceptualize this relationship. That model posits that job demands (such as high workload, emotional demands, and job stress) can lead to exhaustion and disengagement, which may subsequently lead to neglect of job roles such as adherence to cybersecurity protocols. According to the model, high job demands (in the form of job stress) coupled with little control can breed a stress-inducing work environment. Under such stressful circumstances, employees might

inadvertently neglect cybersecurity protocols to cope with their workload, amplifying the vulnerability to cyber threats [43].

Empirical studies have shown that job stress can lead to careless behavior and less adherence to cybersecurity practices. Employees under stress may take shortcuts, ignore policies, or make mistakes, all of which can compromise cybersecurity [44,59].

To summarize, both the General Strain Theory and the Job Demands–Resources model coupled with empirical findings provide a strong theoretical underpinning to argue that job stress could detrimentally affect cybersecurity behavior.

Hypothesis 3. *Job stress negatively affects employee cybersecurity behavior.*

2.4. Job Stress and Work Overload–Cybersecurity Behavior

One of the main purposes of this paper is to investigate the influence of work overload on cybersecurity behavior by identifying the mediating effect of employees' job stress. The central tenet of our research proposes that the association between work overload and cybersecurity behavior can be more precisely delineated by examining the mediating role of job stress. This mediation model is based on the Context–Attitude–Behavior framework, which postulates that the situational context will influence attitude, which in turn determines behavior [60,61]. As such, this study hypothesizes that work overload (context) influences job stress (attitude), which subsequently impacts cybersecurity behavior.

Work overload is a situation wherein work demands exceed the available resources leading to an imbalance that can result in stress [5]. Work overload, in this instance, is the context that causes increased stress levels among employees. Empirical evidence suggests that there is a direct positive correlation between work overload and job stress [11], thus forming the basis for the first part of our mediation hypothesis.

Job stress is an unfavorable emotional response resulting from aspects of work [62], which may have a deleterious impact on cybersecurity behavior. Past research indicates that elevated levels of job stress can compromise employees' adherence to cybersecurity procedures, thereby leading to risky cybersecurity behaviors [63]. As such, this connection between job stress (attitude) and cybersecurity behavior forms the second component of our mediation model.

Given the above, this study posits that job stress serves as a mediator in the relationship between work overload and cybersecurity behavior.

Hypothesis 4. *Employee job stress will mediate the relationship between work overload and cybersecurity behavior.*

2.5. Corporate Ethics and Work Overload–Job Stress

Current research emphasizes the importance of corporate ethics as a critical moderator that buffers the harmful influence of work overload on employees' job stress. While work overload would increase the degree of employee job stress, this influence may not always be the same for all situations, employees, and organizational environments. In other words, various contingent variables, such as employee personality, leadership style, organizational systems, culture, and norms [8,14,16,64] will function as a positive or negative moderator in the association between work overload and job stress. Among the various contextual factors, we focus on the ethical aspects of an organization, specifically corporate ethics.

Corporate ethics, also known as business ethics, is a form of applied ethics that examines ethical principles and moral or ethical problems that arise in a business environment [65]. This concept also refers to the principles, standards, and norms that guide behavior within an organization [66]. It pertains to all aspects of business conduct, and is relevant to the conduct of individuals and entire organizations [67]. These ethics originate from individuals, organizational culture, and the societal context in which a company operates. They set the standards for how a business operates, dictating conduct in various areas like social responsibility, corporate governance, and employee relations [32,67].

In recent years, issues of corporate ethics have gained more attention as stakeholders increasingly hold companies accountable for their actions. A strong corporate ethics framework can enhance reputation, foster loyalty, and drive performance. However, lapses can lead to severe consequences such as legal penalties, reputational damage, and loss of market value [68].

To be specific, we propose that corporate ethics will function as a crucial positive moderator that buffers the harmful effect of work overload on job stress. Corporate ethics can shape individuals' perceptions and interpretations of their work environment, and can potentially moderate the effects of stressors like work overload [69]. When the level of corporate ethics is high, the negative effects of work overload on job stress might be mitigated. Employees in an ethically strong environment may perceive that their workload, while high, is part of a broader organizational mission, rendering it less stressful [70]. For instance, in a healthcare organization, employees often face significant work overload. However, a strong ethical environment that emphasizes patient care and fair treatment can make this workload seem less stressful because employees feel their efforts contribute to a greater good.

Conversely, in organizations with low ethical standards, work overload might more directly lead to job stress. The lack of ethical principles can leave employees feeling unsupported and exploited, amplifying the perceived burden of their workload [71]. An example could be a manufacturing firm where employees are consistently overburdened with long hours and high production targets. If the firm lacks strong ethical values, employees may perceive their workload as unreasonable and exploitative, exacerbating the stress caused by the workload.

Hypothesis 5. *Corporate ethics will diminish the negative effect of work overload on employee job stress by positively moderating the relationship.*

Figure 1 illustrates our theoretical model and all five hypotheses formulated in this section.

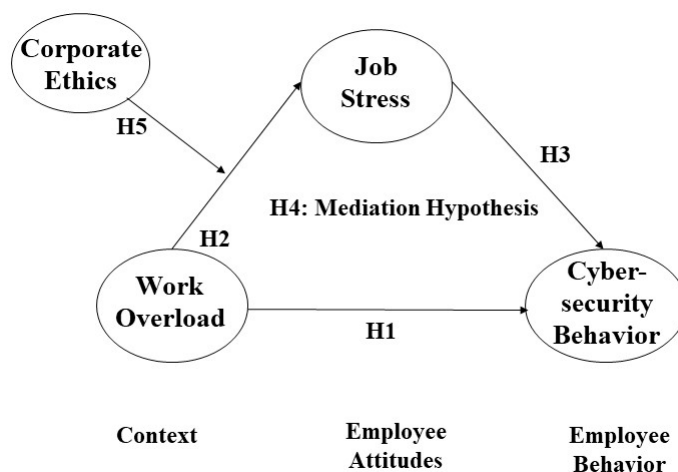


Figure 1. Theoretical model.

3. Method

3.1. Participants and Procedure

The research sample for this study included employed individuals over the age of 20 from several companies in South Korea. Individuals participated at three different points in time. They were recruited by an online research firm with the largest size of available survey participants, comprising approximately 4,270,000 individuals. The respondents reported their occupation status when registering online. The research firm's user authentication system requires participants to share cell phone numbers or email

addresses. The online survey method has been established as a reliable means of accessing a diverse sample of participants.

The information gathered from employees of South Korean companies tried to address the limitations of cross-sectional data. The online system's functions allow researchers to track which members of the dataset participate in a survey, ensuring that participants are the same individuals across separate points in time. Our surveys were conducted at five- to six-week intervals and were opened for two to three days at each time point to allow participants to respond. The company ensured data integrity by utilizing traps to prevent geo-IP violations to flag overly effective responses.

The survey firm reached out directly to its members to request their participation. Researchers assured respondents that their participation would be completely voluntary, and that responses would be kept confidential and used only for this study's purposes. The firm received informed consent and ensured compliance with ethical requirements from those who agreed to participate. They were offered a cash reward of USD 8–9 for their participation.

To minimize sampling bias, the research firm used a stratified random sampling method to select participants. This method drew a random sample from each stratum, reducing bias due to factors such as gender, age, employment position, education, and industry type. The company was able to track respondents through various online systems, ensuring that the participants from each of the three time points were the same (See Table 1).

Table 1. Sample composition.

Variable	Category	Frequency	Percent
Gender	Men	199	52.8%
	Women	178	47.2%
Age (years)	20–29	81	21.5%
	30–39	86	22.8%
	40–49	111	29.4%
	50–59	99	26.3%
	60–69	77	20.4%
Educational Level	High school or below	45	11.9%
	Community college	77	20.4%
	Bachelor's degree	206	54.6%
	Master's degree or higher	49	13.0%
Position	Staff	157	41.6%
	Assistant manager	62	16.4%
	Manager or deputy general manager	92	24.4%
	Department/general manager or director and above	66	17.5%
Industry Type	Manufacturing	81	21.5%
	Services	63	17.8%
	Construction	41	10.9%
	Health and welfare	59	15.6%
	Information services and telecommunications	36	9.5%
	Education	57	15.1%
	Financial/insurance	8	2.1%
	Consulting and advertising	3	0.8%
	Others	29	7.7%

During the first time period (March 2023), 731 employees took part in the survey; the second time (April 2023), 515 employees participated; and during the third time period (May 2023), 379 employees responded. The data were then cleaned by removing surveys with incomplete information. The final sample was 377 participants who fully answered all three surveys (response rate: 51.57%). The sample size was determined by considering various recommendations from prior research, such as checking for sample size suitability using G*Power statistical analysis, and ensuring a minimum sample size of 10 cases per variable, as suggested by Barclay, Higgins, and Thompson [72].

Lastly, our three-wave time-lagged research design was employed to overcome potential limitations in existing studies by providing a more robust and accurate assessment of causal relationships between variables. This design involves collection of data at three distinct time points, allowing researchers to analyze temporal precedence and control for confounding factors while accounting for potential bidirectional or reciprocal relationships between the variables of interest. By establishing clear sequential ordering, this design mitigates the limitations associated with cross-sectional design, which often struggles to disentangle causality and may suffer from common method bias. Furthermore, the three-wave design offers a more nuanced understanding of the causal processes underlying the relationships between variables, thereby enhancing the internal validity and generalizability of the findings, which ultimately contributes to a more rigorous and reliable body of scientific knowledge.

3.2. Measures

Initially, levels of work overload and corporate ethics of the participants were assessed, respectively. At the second time point, levels of job stress were evaluated. At the final time point, cybersecurity behaviors of the participants were measured. All variables were assessed using multi-item, five-point Likert scales. We checked the outliers and normality of the items used in the present study. To be specific, we manually removed the outliers such as the cases that were not included in the range of 1–5 (Likert scale). Also, we performed normality tests including Kolmogorov–Smirnov, Shapiro–Wilk, skewness, and kurtosis. First, as you can see in the below table, the result of the Kolmogorov–Smirnov and Shapiro–Wilk tests indicate that all variables have normality. Second, the absolute value of both skewness and kurtosis showed that all variables were smaller than 0.6, indicating that our data has normality.

In empirical research, particularly when dealing with psychometric evaluations, ensuring the reliability of the instruments used is paramount. Reliability, in this context, refers to the consistency and stability of the scores obtained from these instruments. Among the numerous metrics available to assess reliability, Cronbach's alpha (α) is perhaps the most widely recognized and used, especially in the context of scales with multiple items. Cronbach's alpha is essentially a measure of internal consistency. The rationale behind this metric is that if a set of items pertains to a common latent construct or factor, they should yield similar or consistent scores. A higher alpha value, typically above 0.70, suggests that the items in the scale are closely related and are likely measuring the same underlying construct.

We acknowledge that it is pivotal to test whether the computation of Cronbach's alpha should operate under the assumption of tau-equivalence. This implies that each item in a given scale has the same true score variance and the same error variance (Lord & Novick, 2008 [73]). In other words, it assumes that all items are equally reliable and contribute equivalently to the measured construct. The inclusion of Cronbach's alpha and the testing of tau-equivalence are not mere statistical formalities, they are critical steps in affirming the methodological rigor of our study. By attending to these aspects, we ensure that our findings are built on a foundation of reliable measures, thereby enhancing the validity and generalizability of our research outcomes. We checked the tau-equivalence assumption was satisfied in case of all variables.

3.2.1. Work Overload (Time Point 1)

To gauge the extent of an employee's workload, we utilized five items from established scales [32,74]. Examples of items in our study include "I have unachievable deadlines", "I have to work very fast", "I have to work very intensively", and "I have unrealistic time pressures". Cronbach's alpha was 0.92.

3.2.2. Corporate Ethics (Time Point 1)

To assess the degree of corporate ethics, we utilized four items by adapting them from previous studies [29,75,76]. Sample items are “Our company relies on a code of conduct or ethical standards that define appropriate behavior for its members when making decisions” and “Our company has an organization and systems in place to communicate risk-related information and behaviors that employees should avoid”. Cronbach’s alpha was 0.86.

3.2.3. Job Stress (Time Point 2)

To evaluate the degree of job stress, we utilized four items for the job stress scale by adapting them from scales in previous studies [77,78]. Sample items are “At work, I felt stressed during the last 30 days”, “At work, I felt anxious during the last 30 days”, and “At work, I felt frustrated during the last 30 days”. Cronbach’s alpha was 0.90.

3.2.4. Cybersecurity Behavior (Time Point 3)

This study used six items from cybersecurity behavior scales utilized in previous work [37,41,79,80]. Cronbach’s alpha was 0.87.

3.2.5. Control Variables

Taking into account recommendations from prior research [37,79,80], this study accounted for the effects of cybersecurity behavior by including control variables like tenure, gender, position, and education. These variables were collected during time point 1.

3.3. Data Analytic Strategy

An analysis of the Pearson correlation coefficient was carried out using SPSS 26 to determine the connections among the variables. This study followed a two-step approach suggested by Anderson and Gerbing [81] that includes a measurement model and a structural model. To validate the measurement model, confirmatory factor analysis (CFA) was conducted. Finally, to test the structural model, a moderated mediation model analysis was conducted using AMOS 26 and maximum likelihood estimation based on the principles of structural equation modeling.

This study used several goodness-of-fit indices such as the comparative fit index (CFI), the Tucker–Lewis index (TLI), and root mean square error of approximation (RMSEA). According to previous research, acceptable CFI and TLI values are greater than 0.90, while an acceptable RMSEA value is less than 0.06. Additionally, bootstrapping analysis was conducted to determine the significance of the indirect effect [82]. The study used bootstrapping analysis with a 95% bias-corrected confidence interval (CI) to support the mediation hypothesis. If the CI does not include 0, it implies that the indirect effect is statistically significant at the 0.05 level [82].

4. Results

4.1. Descriptive Statistics

Our research found that the variables of work overload, corporate ethics, job stress, and cybersecurity behavior were strongly correlated. The results of the correlation analysis are in Table 2.

Table 2. Correlation among research variables.

	Mean	SD	1	2	3	4	5
1. Gender	0.47	0.50	-				
2. Tenure	65.24	73.12	−0.10	-			
3. WO	2.65	0.88	−0.15 **	−0.04	-		
4. CE	3.28	0.73	0.00	0.24 **	−0.004	-	
5. JS	2.87	0.84	0.00	−0.11 *	0.40 **	−0.12 *	-
6. CB	3.66	0.72	0.02	0.13 *	−0.12 *	0.26 **	−0.26 **

Notes: * $p < 0.05$. ** $p < 0.01$. SD = standard deviation, WO = work overload, CE = corporate ethics, JS = job stress, CB = cybersecurity behavior. Under gender, male was coded 0, female, 1.

4.2. Measurement Model

This study tested the discriminant validity of the main research variables (work overload, corporate ethics, job stress, and cybersecurity behavior) by conducting CFA of all items to assess the goodness of fit of the measurement model. A series of chi-square difference tests were conducted by comparing the four-factor model (work overload, corporate ethics, job stress, and cybersecurity behavior) to three-factor (χ^2 (df = 178) = 999.407, CFI = 0.820, TLI = 0.787, and RMSEA = 0.111), two-factor (χ^2 (df = 1680) = 1531.565, CFI = 0.703, TLI = 0.654, and RMSEA = 0.141), and one-factor (χ^2 (df = 181) = 2330.866, CFI = 0.528, TLI = 0.452, and RMSEA = 0.178) models. The fit indices of each factor model showed that the four-factor model had a better fit than the other models: χ^2 (df = 175) = 322.218, CFI = 0.968, TLI = 0.961, and RMSEA = 0.047. The results of sequential chi-square difference tests confirmed that our four research variables possess proper discriminant validity.

4.3. Structural Model

A moderated mediation model was constructed to examine the relationship between work overload and cybersecurity behavior. The model included both mediation and moderation structures. In the mediation structure, the impact of work overload on cybersecurity behavior was sequentially mediated by the degree of job stress. In the moderation structure, corporate ethics served as a mitigating variable that reduced the negative effect of work overload on job stress.

In the moderation structure, the interaction term between work overload and corporate ethics was created by multiplying the two variables. To reduce the impact of multicollinearity, the variables were first centered on the mean. This centering process not only decreased the extent of multicollinearity but also reduced loss of correlation, thereby enhancing the validity of the moderation analysis [83].

Due to the self-reported data, there may be a potential issue over common method bias resulting from multiple sources such as social desirability [83]. Based on advice from previous research [83], we implemented statistical analyses to evaluate how serious common method bias might be. First, we performed a Harman's one factor test for all research variables (work overload, corporate ethics, job stress, and cybersecurity behavior). The results showed that the four factors were present, and the highest covariance explained by one factor was 27.91%, meaning that common method bias is not an issue [83].

To assess the influence of multicollinearity bias, this study measured the values for variance inflation factor (VIF) and tolerances [83]. The VIF value for both work overload and corporate ethics was 1.000. The tolerance value was also 1.000 for both work overload and corporate ethics. These results show that work overload and corporate ethics were relatively unaffected by the issue of multicollinearity because VIF values were below 10, and tolerance values were above 0.2.

4.3.1. Results of the Mediation Analysis

A chi-square difference test was conducted to compare a full mediation model and a partial mediation model. The full mediation model was similar to the partial mediation model except for the direct connection between work overload and cybersecurity behavior. Both the full mediation model and the partial mediation model showed acceptable fit, as indicated by the fit indices: χ^2 = 403.181 (df = 210), CFI = 0.953, TLI = 0.943, and RMSEA = 0.049 for the full model, and χ^2 = 403.052 (df = 209), CFI = 0.953, TLI = 0.943, and RMSEA = 0.050 for the partial model.

However, the results of the chi-square difference test revealed that the full mediation model was more adequate. Despite the additional direct path between work overload and cybersecurity behavior, the chi-square value of the partial mediation model did not improve significantly from the full mediation model ($\Delta\chi^2$ [1] = 0.129, $p > 0.05$, non-significant). This suggests that work overload had an indirect effect, rather than a direct effect, on cybersecurity behavior through the mediating factor of job stress.

The study model also included control variables for cybersecurity behavior, such as tenure, gender, education, and position. The results revealed that none of the control variables was statistically significant.

Our research model revealed that work overload's direct effect on cybersecurity behavior is insignificant, rejecting Hypothesis 1. The coefficient value for the path from work overload to cybersecurity behavior in our partial mediation model was $\beta = -0.016$ ($p > 0.05$). This result supports the superiority of the full mediation model relative to the partial mediation model because it showed better fit indices. Based on the results of the comparison between the full and partial mediation models, as well as the insignificant path coefficient from work overload to cybersecurity behavior, we reject Hypothesis 1. The result indicates that the influence of work overload on cybersecurity behavior is likely indirect (through mediating factors such as job stress) rather than direct.

The results support Hypotheses 2 and 3, showing that work overload had a significant and increasing impact on job stress ($\beta = 0.41$, $p < 0.001$), and that job stress had a significant and negative influence on cybersecurity behavior ($\beta = -0.26$, $p < 0.001$). These findings are listed in Table 3 and illustrated in Figure 2.

Table 3. Results of the structural model.

Hypothesis	Path (Relationship)	Unstandardized Estimate	S.E.	Standardized Estimate	Supported
1	Work overload $\rightarrow$ Cybersecurity Behavior	−0.016	0.045	−0.023	No
2	Work overload $\rightarrow$ Job Stress	0.357	0.048	0.405 ***	Yes
3	Job Stress $\rightarrow$ Cybersecurity Behavior	−0.212	0.048	−0.262 ***	Yes
5	Work overload $\times$ Corporate Ethics	−0.249	0.053	0.232 ***	Yes

Notes: *** $p < 0.05$. Estimate indicates standardized coefficients. S.E. means standard error. The coefficient value of the path from work overload to cybersecurity behavior (H1) was in the partial mediation model, which was not accepted as the final model.

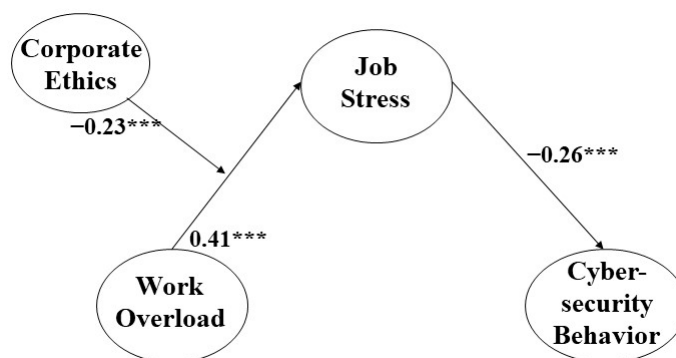


Figure 2. Coefficient values of our research model (*** $p < 0.001$; all values standardized).

4.3.2. Bootstrapping

To verify Hypothesis 4, which states that job stress will mediate the relationship between work overload and cybersecurity behavior, this study conducted bootstrapping analysis on 10,000 samples by following the method described by Shrout and Bolger [82]. The indirect effect of job stress is considered statistically significant if the 95% bias-corrected confidence interval for the mean indirect effect does not include zero [82].

Bootstrapping analysis on 10,000 samples tested the mediation impact of job stress in the work overload–cybersecurity behavior link (Hypothesis 4). The indirect mediation effect would be considered significant if the 95% bias-corrected CI for the mean indirect mediation effect does not include 0. Our results indicate that the CI excluded zero (95% CI = [−0.172, −0.052]), demonstrating that the indirect mediation impact of job stress was statistically significant, supporting Hypothesis 4. Table 4 presents the direct, indirect, and total effect of the paths from work overload to cybersecurity behavior.

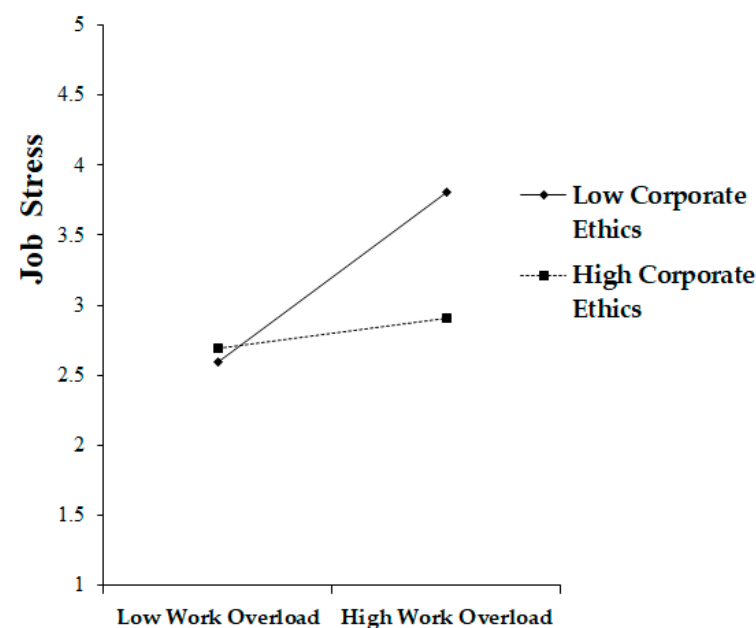
Table 4. Direct, indirect, and total effects of the final research model.

Model (Hypothesis 4)	Direct Effect	Indirect Effect	Total Effect
Work overload → Job Stress → Cybersecurity Behavior	0.000	0.106	−0.106

Note: All values are standardized.

4.3.3. Result of Moderation Analysis

This study examines the moderating impact of corporate ethics on the work overload–job stress link. This was performed by creating an interaction term between work overload and corporate ethics through a mean-centering process. The results show that the interaction term was significant ($\beta = 0.20$, $p < 0.01$), indicating that corporate ethics plays a positive moderating role in buffering the increasing effect of work overload on job stress. This supports Hypothesis 5 (Refer to Figure 3).

**Figure 3.** Moderating effect of corporate ethics in the work overload–job stress link.

5. Discussion

This study set out with the objective of exploring the intricate dynamics of work overload, job stress, and organizational ethics, and their collective influence on employees' cyber security behavior. Our findings have provided important insights into this multi-faceted relationship, yet it is essential to juxtapose these results with the existing literature and acknowledge the limitations that have surfaced during the course of this research.

The direct relationship established between work overload and decreased cyber security behavior among employees is consistent with the broader literature on the implications of work overload [5–16]. While several previous works found a negative correlation between work overload and job satisfaction, organizational commitment, self-esteem, intrinsic motivation, organizational identification, and job performance [7–14], our study adds a dimension by linking work overload to a crucial organizational behavior–cybersecurity behavior [22]. This indicates that the ramifications of work overload extend beyond traditional measures of employee well-being, permeating into areas of operational significance [9,10]. While the broader academic corpus has established the negative implications of work overload on various organizational outcomes, its impact on cyber security behavior has been less charted. Previous research discussed work overload in the context of diminished employee organizational commitment, job satisfaction, and organizational citizenship behavior [7–13]. This study, in contrast, extends the narrative by demonstrating that the

implications of work overload reach areas of operational exigency, particularly cyber security. Such a discovery fills a significant gap, highlighting the multi-faceted repercussions of work overload in the digital age.

The mediating role of job stress, though inferred in various studies examining job stress outcomes [50–54], found a more explicit manifestation in our research. It was intriguing to observe that the adverse consequences of work overload on cyber security behavior were largely channeled through increased job stress, reinforcing the centrality of job stress in discussions around organizational efficiency and security [9,10,22]. To be specific, various studies, including that Karimi et al. [32] have touched upon the outcomes stemming from job stress. However, the explicit elucidation of job stress as a conduit between work overload and cyber security behavior is a novel contribution from this research. While Karimi and colleagues discussed job stress outcomes in broader contexts, our study narrows down the focus, emphasizing the centrality of job stress in discussions specific to cyber security outcomes.

Furthermore, our exploration of the buffering role of organizational ethics provides an essential addition to the literature. While some scholars [65–67] highlighted the influence of organizational ethics on individual decision making, our research positions organizational ethics as a potential safeguard against the detrimental effects of work overload. This understanding underscores the importance of fostering a strong ethical culture in organizations, not merely for moral uprightness but also for practical benefits in the realm of cyber security. To be specific, the realm of organizational ethics has predominantly been linked to individual decision making, as put forth by Koh and his colleagues [66]. However, their study centered more on the broader influences of organizational ethics on decision-making patterns. Our research, diverging from this path, accentuates the role of organizational ethics as a potential bulwark against the adverse effects of work overload on cyber security behavior. This is a significant shift from the general discussions around ethical culture, positioning organizational ethics as a tangible mitigator in the face of operational challenges.

What sets this study apart is its nuanced approach to understanding a contemporary issue that holds pronounced relevance in today's digitized work environments. By intricately weaving the constructs of work overload, job stress, and organizational ethics, and linking them to cyber security behavior, this research provides a holistic lens to fathom the intricate interdependencies between these variables. It is this depth of examination, backed by robust methodologies, that renders the study invaluable, filling the gaps left by prior works and offering fresh perspectives for scholars and practitioners alike.

In summary, this study makes meaningful strides towards a more comprehensive understanding of the factors affecting cybersecurity behavior in the context of work overload. It provides both theoretical and practical insights for scholars, practitioners, and policymakers alike, underscoring the need for further research in this critical area of study.

In the contemporary digital epoch, as organizations grapple with the incessant challenges posed by cyber threats, the onus of understanding the antecedents of cybersecurity behaviors has never been more pressing. While myriad studies have delved into the technical and procedural elements of cybersecurity, a significant lacuna persists in comprehending the human-centric factors that underpin these behaviors. This research, therefore, embarked on a pivotal journey to fill this scholarly void, elucidating the intricate nexus between work overload, job stress, and cybersecurity behaviors.

Central to our exploration was the assertion that work overload—a prevalent phenomenon in modern workspaces—plays a crucial role in shaping cybersecurity behaviors. Contrary to the prevalent focus on merely technical aspects, this research underscored that the implications of work overload transcend mere productivity concerns and profoundly infiltrate the domain of cybersecurity. By delineating the mediating role of job stress and the moderating influence of organizational ethics, our study illuminates the multifaceted pathways through which workload pressures can either compromise or bolster cybersecurity practices.

Furthermore, in an era where digital interconnectivity has become the linchpin of organizational operations, the ramifications of neglecting such human-induced vulnerabilities can be dire. This research, therefore, not only fills a glaring gap in the academic literature but also accentuates a pressing concern for practitioners. By demystifying how work dynamics, especially work overload, cascade into the realm of cybersecurity behaviors, this investigation offers both scholars and practitioners a nuanced perspective, urging them to recalibrate their cybersecurity strategies in alignment with the human elements of the organizational tapestry. This research stands as a testament to the pivotal role of human factors in cybersecurity, reiterating the need for a harmonized approach that integrates technical, procedural, and human-oriented strategies to fortify digital defenses in today's interconnected landscape.

5.1. Theoretical Implications

The findings of this study have several important theoretical implications for the research community, particularly for those investigating work overload, job stress, corporate ethics, and cybersecurity behavior.

First, this study advances the discourse on work overload by theorizing and demonstrating its potential impacts on cybersecurity behavior. The prevailing understanding of work overload mainly revolves around its association with variables such as job satisfaction, turnover intention, and burnout [84]. Our study expands this perspective by establishing a novel linkage between work overload and cybersecurity behavior. By illustrating the linkage between work overload and cyber security behavior, mediated by job stress, this study carves out a comprehensive theoretical landscape, urging scholars to view work overload as not just an individual or psychological construct, but one with cascading operational implications, particularly in the realm of cyber security. Hence, this research provides a valuable lens to understand the broader implications of work overload in today's digitalized work context.

Second, this study significantly contributes to stress research by elucidating the mediating role of job stress on the relationship between work overload and cybersecurity behavior. Although existing studies documented various outcomes of job stress, an understanding of its influence on cybersecurity behavior is lacking [85]. Historically, the discourse around job stress was centered on its antecedents and immediate repercussions. This study's emphasis on its mediating role provides an enriched theoretical perspective. It underscores that job stress does not merely arise from precursors like work overload, but it can serve as a pivotal mechanism that transmits the effects of such precursors onto crucial organizational outcomes, in this case, cyber security behavior. By identifying job stress as a critical mediator, this study enriches the literature on stress with a novel insight.

Third, finding a moderating role from corporate ethics offers fresh theoretical insights on the importance of ethical climate in the stress process. The extant research has mostly focused on individual-level moderators such as personality traits or coping strategies [29]. By demonstrating the buffering role of corporate ethics, this study prompts researchers to consider the influence of organizational-level factors in stress research. Furthermore, theoretical discussions around organizational ethics have largely been normative, delving into its foundational principles and ethical decision-making paradigms. This study pushes the envelope by highlighting the buffering potential of organizational ethics. Such a perspective nudges theoretical frameworks to accommodate organizational ethics not just as a determinant of moral decisions, but also as a potential moderator, capable of influencing how other organizational variables interact and translate into tangible outcomes.

Finally, the integration of work overload, job stress, and corporate ethics in a single model promotes a comprehensive understanding of cybersecurity behavior. To be specific, one of the profound theoretical insights emanating from this study is the integrative potential of the aforementioned constructs. When work overload, job stress, and organizational ethics are studied in tandem, they offer a richer, more layered understanding, illuminating the nuanced interplay between these elements. Scholars are thus presented with a cohesive

framework, which can serve as a launchpad for more intricate, interconnected explorations in the domain. Despite the increasing prevalence of cybersecurity issues, research on this topic is still in its infancy [23]. This study contributes to this emerging field by offering a multi-level framework that can serve as a foundation for future investigations.

5.2. Practical Implications

The results of this investigation unveil several pivotal practical implications, furnishing top management teams, leaders, and employees with a more refined understanding of the interplay between work overload, job stress, organizational ethics, and cyber security behavior.

First, by demonstrating the link between work overload and cybersecurity behavior, our research suggests that organizations need to be cautious about overloading employees with excessive tasks. Recognizing the direct and indirect influences of work overload on cyber security behavior through job stress paves the way for more informed management decisions. Top management teams should prioritize workload management not merely to boost productivity or employee well-being but also as a strategic lever to enhance cyber security practices. Interventions such as workload balancing, delegation, and time management training can thus serve dual purposes—promoting employee well-being and fortifying cyber resilience. Given the increasing dependency on digital technology, the risk of cybersecurity breaches has become a major concern for organizations worldwide [23]. Therefore, organizations must monitor and manage work overload to minimize the potential risk from cybersecurity threats.

Second, our study sheds light on the significance of managing job stress in order to promote cybersecurity behavior. Previous research has long stressed the need to manage job stress due to its detrimental effects on employee health and productivity [85]. Our study further emphasizes this need by uncovering its critical role in shaping cybersecurity behavior. With the revelation that job stress mediates the link between work overload and cyber security behavior, organizations have a compelling reason to invest in stress-relief and mental well-being programs. Leaders can view these initiatives as not just employee support mechanisms but also as crucial components of the broader cyber security strategy. Techniques like mindfulness training, flexible working conditions, and regular breaks can be incorporated to alleviate stress, indirectly promoting better cyber hygiene among employees.

Third, finding the buffering role of corporate ethics provides insights for organizational policy making. The moderating effect of organizational ethics offers a potent tool for leaders. Rather than seeing ethics as a passive set of principles, leaders can actively deploy organizational ethics as a buffer against the potentially negative spill-overs of work overload. By instilling a strong ethical foundation, organizations can reduce the likelihood that overloaded employees resort to shortcuts or unsafe practices that jeopardize cyber security. Ethical training, transparent communication, and leadership by example can be effective strategies in this regard. As our study suggests, fostering an ethical climate can mitigate the negative impacts of work overload on job stress. Therefore, organizations could consider enhancing their ethical climate by implementing a strong code of ethics, encouraging ethical leadership, and promoting ethical training programs [29].

Finally, with the integrative understanding of work overload, stress, and ethics, employee training modules can be designed more holistically. Instead of isolated training on workload management or cyber security best practices, a comprehensive curriculum can be devised. Such an integrated training can help employees understand the interconnections between their workload, the resultant stress, the organization's ethical stance, and the imperatives of cyber security, leading to more informed and responsible behaviors.

In essence, the practical insights drawn from this study provide a roadmap for organizations. By interweaving the understanding of work overload, job stress, and organizational ethics, top management teams, leaders, and employees are equipped with a holistic toolkit,

ensuring not just optimal performance and well-being, but also robust cyber security behaviors in the face of evolving digital challenges.

5.3. Limitations and Suggestions for Future Studies

While this study advances our understanding of work overload, job stress, and cybersecurity behavior in the organizational setting, it is not without limitations.

First, the study relies on a cross-sectional design, which makes it difficult to make causal inferences between work overload, job stress, and cybersecurity behavior. Although we theoretically argue for directional relationships, future research could benefit from employing a longitudinal design to better capture the dynamics and causality among these variables [86].

Second, we used self-reported measures for all the constructs, which might have led to common method bias [87]. Although self-reports are commonly used in organizational research, future studies could triangulate our findings with other data sources, such as supervisor ratings or behavioral observation, to minimize potential bias.

Third, while we highlight the moderating role of corporate ethics, we acknowledge that other contextual factors could also impact the relationships in our model. For instance, organizational culture, leadership style, or technological infrastructure might play a role [88]. Future research could consider examining the interplay of these factors with work overload and job stress on cybersecurity behavior.

Finally, this study focused on the Context–Attitude–Behavior framework, and while that model offers robust theoretical grounds for our arguments, there are other theoretical lenses through which the relationships could be viewed, such as the Job Demands–Resources model [58] or Conservation of Resources theory [45]. Future research is encouraged to apply these or other theoretical perspectives to offer a more comprehensive understanding of cybersecurity behavior.

6. Conclusions

This study endeavored to contribute to the literature by elucidating the intricate relationships between work overload, job stress, and cybersecurity behavior. Through the lens of the Context–Attitude–Behavior framework, we offer a nuanced understanding of how work overload could influence employees' cybersecurity behavior, and the vital role that job stress plays as a mediating factor in this relationship. Moreover, we highlighted the significance of corporate ethics as a potential moderating variable, buffering the adverse effects of work overload on job stress that ultimately affects cybersecurity behavior. By integrating these elements, our research provides a more comprehensive picture of the critical factors impacting cybersecurity behavior in the workplace.

Theoretically, this research challenges existing paradigms and broadens the academic lens, advocating for a more holistic understanding of cybersecurity. By interweaving work overload and job stress into the cybersecurity discourse, we not only unearth novel insights but also push theoretical boundaries. The nuanced role of organizational ethics as a moderating factor further enriches this discourse, accentuating the intricate balance between workplace pressures and ethical frameworks in shaping cybersecurity behaviors. Thus, our study paves the way for a new wave of interdisciplinary research, beckoning scholars to explore this confluence of work dynamics and cybersecurity further.

From a practical standpoint, our findings serve as a clarion call for organizations, urging them to acknowledge and address the ramifications of work overload. In an era where cyber threats loom large, the significance of understanding and mitigating human-induced vulnerabilities is paramount. Leaders, top management teams, and employees can draw upon our insights to foster a work environment that not only mitigates stress but also fortifies its digital bastions. The revelations about the buffering role of organizational ethics further offer organizations a roadmap to instill a robust ethical fabric, one that can potentially shield them from the inadvertent cybersecurity lapses that arise from work-related pressures.

In closing, while our study provides a substantial leap forward, it also lays the foundation for future inquiries. As we stand on the cusp of a digital revolution, understanding the myriad ways in which human factors intertwine with cybersecurity becomes not just relevant, but imperative. Our research, therefore, serves as both a culmination of rigorous investigation and an initiation—a beacon that lights the path for future studies, beckoning them to delve deeper into this uncharted confluence.

Author Contributions: Conceptualization, Y.H., M.-J.K. and T.R.; Methodology, Y.H. and T.R.; Software, M.-J.K.; Validation, M.-J.K. and T.R.; Formal analysis, Y.H.; Writing—original draft, Y.H.; Writing—review & editing, M.-J.K. and T.R.; Supervision, M.-J.K. and T.R.; Project administration, M.-J.K. and T.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board of Yonsei University (protocol code: 202208-HR-2975-01, and date of approval: 15 August 2022).

Informed Consent Statement: Informed consent was obtained from all the participants.

Data Availability Statement: New data were created and analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sergent, K.; Stajkovic, A.D. Women's leadership is associated with fewer deaths during the COVID-19 crisis: Quantitative and qualitative analyses of United States governors. *J. Appl. Psychol.* **2020**, *105*, 771. [\[CrossRef\]](#)
2. Spurk, D.; Straub, C. Flexible employment relationships and careers in times of the COVID-19 pandemic. *J. Vocat. Behav.* **2020**, *119*, 103435. [\[CrossRef\]](#)
3. Caplan, R.D.; Jones, K.W. Effects of work load, role ambiguity, and Type A personality on anxiety, depression, and heart rate. *J. Appl. Psychol.* **1975**, *60*, 713–719. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Carr, J.C.; Marshall, D.R.; Michaelis, T.L.; Pollack, J.M.; Sheats, L. The role of work-to-venture role conflict on hybrid entrepreneurs' transition into entrepreneurship. *J. Small Bus. Manag.* **2023**, *61*, 2302–2325. [\[CrossRef\]](#)
5. Bakker, A.B.; Demerouti, E.; Euwema, M.C. Job resources buffer the impact of job demands on burnout. *J. Occup. Health Psychol.* **2005**, *10*, 170–180. [\[CrossRef\]](#) [\[PubMed\]](#)
6. Mhango, M.; Dzobo, M.; Chitungo, I.; Dzinamarira, T. COVID-19 risk factors among health workers: A rapid review. *Saf. Health Work* **2020**, *11*, 262–265. [\[CrossRef\]](#) [\[PubMed\]](#)
7. Kumar, S.; Hansiya Abdul Rauf, F.; Rathnasekara, H. Working to help or helping to work? Work-overload and allocentrism as predictors of organizational citizenship behaviours. *Int. J. Hum. Resour. Manag.* **2021**, *32*, 2807–2828. [\[CrossRef\]](#)
8. Barriga Medina, H.R.; Campoverde Aguirre, R.; Coello-Montecel, D.; Ochoa Pacheco, P.; Paredes-Aguirre, M.I. The influence of work–family conflict on burnout during the COVID-19 pandemic: The effect of teleworking overload. *Int. J. Environ. Res. Public Health* **2021**, *18*, 10302. [\[CrossRef\]](#)
9. Odes, R.; Hong, O. Job Stress and Sleep Disturbances among Career Firefighters in Northern California. *J. Occup. Environ. Med.* **2023**, *68*, 706–710.
10. Hon, A.H.; Kim, T.Y. Work overload and employee creativity: The roles of goal commitment, task feedback from supervisor, and reward for competence. *Curr. Top. Manag.* **2018**, *12*, 193–211.
11. Izdebski, Z.; Kozakiewicz, A.; Białorudzki, M.; Dec-Pietrowska, J.; Mazur, J. Occupational burnout in healthcare workers, stress and other symptoms of work overload during the COVID-19 pandemic in Poland. *Int. J. Environ. Res. Public Health* **2023**, *20*, 2428. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Kmiecik, R. Knowledge-withholding behaviours among IT specialists: The roles of job insecurity, work overload and supervisor support. *J. Manag. Organ.* **2023**, *29*, 383–399. [\[CrossRef\]](#)
13. Hwang, Y.S.; Kim, B.J. "The Power of a Firm's Benevolent Act": The Influence of Work Overload on Turnover Intention, the Mediating Role of Meaningfulness of Work and the Moderating Effect of CSR Activities. *Int. J. Environ. Res. Public Health* **2021**, *18*, 3780. [\[CrossRef\]](#) [\[PubMed\]](#)
14. Ingusci, E.; Signore, F.; Giancaspro, M.L.; Manuti, A.; Molino, M.; Russo, V.; Zito, M.; Cortese, C.G. Workload, techno overload, and behavioral stress during COVID-19 emergency: The role of job crafting in remote workers. *Front. Psychol.* **2021**, *12*, 655148. [\[CrossRef\]](#) [\[PubMed\]](#)
15. Sandoval-Reyes, J.; Acosta-Prado, J.C.; Sanchís-Pedregosa, C. Relationship amongst technology use, work overload, and psychological detachment from work. *Int. J. Environ. Res. Public Health* **2019**, *16*, 4602. [\[CrossRef\]](#) [\[PubMed\]](#)

16. She, Z.; Li, B.; Li, Q.; London, M.; Yang, B. The double-edged sword of coaching: Relationships between managers' coaching and their feelings of personal accomplishment and role overload. *Hum. Resour. Dev. Q.* **2019**, *30*, 245–266. [\[CrossRef\]](#)
17. Mazzetti, G.; Robledo, E.; Vignoli, M.; Topa, G.; Guglielmi, D.; Schaufeli, W.B. Work engagement: A meta-analysis using the job demands-resources model. *Psychol. Rep.* **2023**, *126*, 1069–1107. [\[CrossRef\]](#)
18. Tran, Q.H.N. Exploring relationships among overload stress, work-family conflict, job satisfaction, person–organisation fit and organisational commitment in public organizations. *Public Organ. Rev.* **2023**, *23*, 759–775. [\[CrossRef\]](#)
19. Graf, B.; Antoni, C.H. Drowning in the flood of information: A meta-analysis on the relation between information overload, behaviour, experience, and health and moderating factors. *Eur. J. Work. Organ. Psychol.* **2023**, *32*, 173–198. [\[CrossRef\]](#)
20. Sheng, N.; Yang, C.; Han, L.; Jou, M. Too much overload and concerns: Antecedents of social media fatigue and the mediating role of emotional exhaustion. *Comput. Hum. Behav.* **2023**, *139*, 107500. [\[CrossRef\]](#)
21. Spector, P.E.; Jex, S.M. Development of four self-report measures of job stressors and strain: Interpersonal conflict at work scale, organizational constraints scale, quantitative workload inventory, and physical symptoms inventory. *J. Occup. Health Psychol.* **1998**, *3*, 356–367. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Khan, N.F.; Yaqoob, A.; Khan, M.S.; Ikram, N. The cybersecurity behavioral research: A tertiary study. *Comput. Secur.* **2023**, *120*, 102826. [\[CrossRef\]](#)
23. Alanazi, M.; Freeman, M.; Tootell, H. Exploring the factors that influence the cybersecurity behaviors of young adults. *Comput. Hum. Behav.* **2023**, *136*, 107376. [\[CrossRef\]](#)
24. Alsharida, R.A.; Al-rimy, B.A.S.; Al-Emran, M.; Zainal, A. A systematic review of multi perspectives on human cybersecurity behavior. *Technol. Soc.* **2023**, *73*, 102258. [\[CrossRef\]](#)
25. Almansoori, A.; Al-Emran, M.; Shaalan, K. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Appl. Sci.* **2023**, *13*, 5700. [\[CrossRef\]](#)
26. Kannelønning, K.; Katsikas, S.K. A Systematic literature review of how cybersecurity-related behavior has been assessed. *Inf. Comput. Secur.* **2023**, *in press*. [\[CrossRef\]](#)
27. Khan, N.F.; Ikram, N.; Murtaza, H.; Javed, M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Comput. Secur.* **2023**, *125*, 103049. [\[CrossRef\]](#)
28. Lee, C.S.; Kim, D. Pathways to cybersecurity awareness and protection behaviors in South Korea. *J. Comput. Inf. Syst.* **2023**, *63*, 94–106. [\[CrossRef\]](#)
29. Jammaers, E. Theorizing discursive resistance to organizational ethics of care through a multi-stakeholder perspective on disability inclusion practices. *J. Bus. Ethics* **2023**, *183*, 333–345. [\[CrossRef\]](#)
30. National Institute for Occupational Safety and Health (NIOSH). *Stress at Work*; Publication Number 99–101; NIOSH: Washington, DC, USA, 1999.
31. Lahti, H.; Kalakoski, V. Work stressors and their controllability: Content analysis of employee perceptions of hindrances to the flow of work in the health care sector. *Curr. Psychol.* **2022**, *1–19*. [\[CrossRef\]](#)
32. Karimi, Z.; Haghshenas, L.; Asghari, M.; Teimori, G.; Abedinloo, R. Relationship between Job Stress, Job Satisfaction, and Related Factors among Health Center Employees. *J. Occup. Hyg. Eng.* **2023**, *9*, 259–266. [\[CrossRef\]](#)
33. Mathieu, C.; Gilbreath, B. Measuring Presenteeism from Work Stress: The Job Stress-Related Presenteeism Scale. *J. Occup. Environ. Med.* **2023**, *65*, 210–216. [\[CrossRef\]](#) [\[PubMed\]](#)
34. Muyidi, A.; Zhang, Y.B.; Gist-Mackey, A. The influence of gender discrimination, supervisor support, and government support on Saudi female journalists' job stress and satisfaction. *Manag. Commun. Q.* **2023**, *37*, 207–224. [\[CrossRef\]](#)
35. Farid, G.; Warraich, N.F.; Iftikhar, S. Digital information security management policy in academic libraries: A systematic review (2010–2022). *J. Inf. Sci.* **2023**, 01655515231160026. [\[CrossRef\]](#)
36. Tempestini, G.; Rovira, E.; Pyke, A.; Di Nocera, F. The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. *J. Cybersec. Priv.* **2023**, *3*, 61–75. [\[CrossRef\]](#)
37. Kioskli, K.; Fotis, T.; Nifakos, S.; Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Appl. Sci.* **2023**, *13*, 3410. [\[CrossRef\]](#)
38. Mahlangu, G.; Chipfumbu Kangara, C.; Masunda, F. Citizen-centric cybersecurity model for promoting good cybersecurity behaviour. *J. Cyber Secur. Technol.* **2023**, *7*, 154–180. [\[CrossRef\]](#)
39. Renaud, K.; Dupuis, M. Cybersecurity insights gleaned from world religions. *Comput. Secur.* **2023**, *132*, 103326. [\[CrossRef\]](#)
40. Karasek, R.A. Job demands, job decision latitude, and mental strain: Implications for job redesign. *Adm. Sci. Q.* **1979**, *24*, 285–308. [\[CrossRef\]](#)
41. Kävrestad, J.; Furnell, S.; Nohlberg, M. User perception of Context-Based Micro-Training—a method for cybersecurity training. *Inf. Secur. J. A Glob. Perspect.* **2023**, *1–17*. [\[CrossRef\]](#)
42. De Clercq, D.; Haq, I.U.; Azeem, M.U. Gossiping about outsiders: How time-related work stress among collectivistic employees hinders job performance. *J. Manag. Organ.* **2023**, *29*, 191–206. [\[CrossRef\]](#)
43. Madnick, B.; Huang, K.; Madnick, S. The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Inf. Secur. J. A Glob. Perspect.* **2023**, *1–22*. [\[CrossRef\]](#)
44. Arpaci, I.; Bahari, M. A complementary SEM and deep ANN approach to predict the adoption of cryptocurrencies from the perspective of cybersecurity. *Comput. Hum. Behav.* **2023**, *143*, 107678. [\[CrossRef\]](#)
45. Hobfoll, S.E. Conservation of resources: A new attempt at conceptualizing stress. *Am. Psychol.* **1989**, *44*, 513–524. [\[CrossRef\]](#)

46. Bakker, A.B.; Xanthopoulou, D.; Demerouti, E. How does chronic burnout affect dealing with weekly job demands? A test of central propositions in JD-R and COR-theories. *Appl. Psychol.* **2023**, *72*, 389–410. [\[CrossRef\]](#)
47. Yang, C.; Yang, L.; Wu, D. The influence of grit on nurse job satisfaction: Mediating effects of perceived stress and moderating effects of optimism. *Front. Psychol.* **2023**, *13*, 1094031. [\[CrossRef\]](#)
48. Baum, M.; Sattler, S.; Reimann, M. Towards an understanding of how stress and resources affect the nonmedical use of prescription drugs for performance enhancement among employees. *Curr. Psychol.* **2023**, *42*, 4784–4801. [\[CrossRef\]](#)
49. Bakker, A.B.; Demerouti, E.; Sanz-Vergel, A.I. Burnout and work engagement: The JD–R approach. *Annu. Rev. Organ. Psychol. Organ. Behav.* **2014**, *1*, 389–411. [\[CrossRef\]](#)
50. Sauter, S.L.; Murphy, L.R.; Hurrell, J.J. Prevention of work-related psychological disorders: A national strategy proposed by the National Institute for Occupational Safety and Health (NIOSH). *Am. Psychol.* **1990**, *45*, 1146–1158. [\[CrossRef\]](#)
51. Karasek, R.; Theorell, T. *Healthy Work: Stress, Productivity, and the Reconstruction of Working Life*; Basic Books; Wiley: Hoboken, NJ, USA, 1990.
52. Lazarus, R.S.; Folkman, S. *Stress, Appraisal, and Coping*; Springer Publishing Company: Berlin/Heidelberg, Germany, 1984.
53. De Giorgio, A.; Barattucci, M.; Teresi, M.; Raulli, G.; Ballone, C.; Ramaci, T.; Pagliaro, S. Organizational identification as a trigger for personal well-being: Associations with happiness and stress through job outcomes. *J. Community Appl. Soc. Psychol.* **2023**, *33*, 138–151. [\[CrossRef\]](#)
54. Elomaa, M.; Eskelä-Haapanen, S.; Pakarinen, E.; Halttunen, L.; Lerkkanen, M.K. Work-related stress of elementary school principals in Finland: Coping strategies and support. *Educ. Manag. Adm. Leadersh.* **2023**, *51*, 868–888. [\[CrossRef\]](#)
55. Mauno, S.; Herttälampi, M.; Minkkinen, J.; Feldt, T.; Kubicek, B. Is work intensification bad for employees? A review of outcomes for employees over the last two decades. *Work Stress* **2023**, *37*, 100–125. [\[CrossRef\]](#)
56. Kushner, M.; Fagan, A.A. The effects of victimization on offending: An examination of General Strain Theory, criminal propensity, risk, protection, and resilience. *Vict. Offenders* **2023**, *18*, 1009–1029. [\[CrossRef\]](#)
57. Kim, J.; Leban, L.; Lee, Y.; Jennings, W.G. Testing gender differences in victimization and negative emotions from a developmental general strain theory perspective. *Am. J. Crim. Justice* **2023**, *48*, 444–462. [\[CrossRef\]](#)
58. Demerouti, E.; Bakker, A.B. Job demands-resources theory in times of crises: New propositions. *Organ. Psychol. Rev.* **2023**, *13*, 209–236. [\[CrossRef\]](#)
59. Bakker, A.B.; Demerouti, E.; Sanz-Vergel, A. Job demands–resources theory: Ten years later. *Annu. Rev. Organ. Psychol. Organ. Behav.* **2023**, *10*, 25–53. [\[CrossRef\]](#)
60. Mulki, J.P.; Jaramillo, J.F.; Locander, W.B. Critical role of leadership on ethical climate and salesperson behaviors. *J. Bus. Ethics* **2009**, *86*, 125–141. [\[CrossRef\]](#)
61. Kaptein, M. A paradox of ethics: Why people in good organizations do bad things. *J. Bus. Ethics* **2023**, *184*, 297–316. [\[CrossRef\]](#)
62. Martí-González, M.; Alcalá-Ibañez, M.L.; Castán-Esteban, J.L.; Martín-Bielsa, L.; Gallardo, L.O. COVID-19 in school teachers: Job satisfaction and burnout through the job demands control model. *Behav. Sci.* **2023**, *13*, 76. [\[CrossRef\]](#)
63. Posey, C.; Roberts, T.L.; Lowry, P.B. The impact of organizational commitment on insiders’ motivation to protect organizational information assets. *J. Manag. Inf. Syst.* **2015**, *32*, 179–214. [\[CrossRef\]](#)
64. Jeong, J.; Kim, B.J.; Kim, M.J. The impact of job insecurity on knowledge-hiding behavior: The mediating role of organizational identification and the buffering role of coaching leadership. *Int. J. Environ. Res. Public Health* **2022**, *19*, 16017. [\[CrossRef\]](#)
65. Trittin-Ulbrich, H. From the substantive to the ceremonial: Exploring interrelations between recognition and aspirational CSR talk. *Bus. Soc.* **2023**, *62*, 917–949. [\[CrossRef\]](#)
66. Koh, K.; Li, H.; Tong, Y.H. Corporate social responsibility (CSR) performance and stakeholder engagement: Evidence from the quantity and quality of CSR disclosures. *Corp. Soc. Responsib. Environ. Manag.* **2023**, *30*, 504–517. [\[CrossRef\]](#)
67. Fatima, T.; Elbanna, S. Corporate social responsibility (CSR) implementation: A review and a research agenda towards an integrative framework. *J. Bus. Ethics* **2023**, *183*, 105–121. [\[CrossRef\]](#) [\[PubMed\]](#)
68. Cao, S.; Yao, H.; Zhang, M. CSR gap and firm performance: An organizational justice perspective. *J. Bus. Res.* **2023**, *158*, 113692. [\[CrossRef\]](#)
69. Ahmad, W.; Jafar, R.M.S.; Waheed, A.; Sun, H.; Kazmi, S.S.A.S. Determinants of CSR and green purchase intention: Mediating role of customer green psychology during COVID-19 pandemic. *J. Clean. Prod.* **2023**, *389*, 135888. [\[CrossRef\]](#) [\[PubMed\]](#)
70. Battisti, E.; Nirino, N.; Leonidou, E.; Salvi, A. Corporate social responsibility in family firms: Can corporate communication affect CSR performance? *J. Bus. Res.* **2023**, *162*, 113865. [\[CrossRef\]](#)
71. Guan, X.; Ahmad, N.; Sial, M.S.; Cherian, J.; Han, H. CSR and organizational performance: The role of pro-environmental behavior and personal values. *Corp. Soc. Responsib. Environ. Manag.* **2023**, *30*, 677–694. [\[CrossRef\]](#)
72. Collier, J. *Applied Structural Equation Modeling Using AMOS: Basic to Advanced Techniques*; Routledge: Oxfordshire, UK, 2020.
73. Lord, F.M.; Novick, M.R.; Birnbaum, A. *Statistical Theories of Mental Test Scores*; Information Age Publishing: Charlotte, CA, USA, 2008.
74. Cousins, R.; Mackay, C.J.; Clarke, S.D.; Kelly, C.; Kelly, P.J.; McCaig, R.H. ‘Management standards’ work-related stress in the UK: Practical development. *Work. Stress* **2004**, *18*, 113–136. [\[CrossRef\]](#)
75. Chun, J.S.; Shin, Y.; Choi, J.N.; Kim, M.S. How does corporate ethics contribute to firm financial performance? The mediating role of collective organizational commitment and organizational citizenship behavior. *J. Manag.* **2013**, *39*, 853–877.
76. Victor, B.; Cullen, J.B. The organizational bases of ethical work climates. *Adm. Sci. Q.* **1988**, *33*, 101–125. [\[CrossRef\]](#)

77. DeJoy, D.M.; Wilson, M.G.; Vandenberg, R.J.; McGrath-Higgins, A.L.; Griffin-Blake, C.S. Assessing the impact of healthy work organization intervention. *J. Occup. Organ. Psychol.* **2010**, *83*, 139–165. [[CrossRef](#)]
78. Motowidlo, S.J.; Packard, J.S.; Manning, M.R. Occupational stress: Its causes and consequences for job performance. *J. Appl. Psychol.* **1986**, *71*, 618. [[CrossRef](#)]
79. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [[CrossRef](#)]
80. Padayachee, K. Taxonomy of compliant information security behavior. *Comput. Secur.* **2012**, *31*, 673–680. [[CrossRef](#)]
81. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411–423. [[CrossRef](#)]
82. Shrout, P.E.; Bolger, N. Mediation in experimental and nonexperimental studies: New procedures and recommendations. *Psychol. Methods* **2002**, *7*, 422–445. [[CrossRef](#)] [[PubMed](#)]
83. Brace, N.; Kemp, R.; Snelgar, R. *A Guide to Data Analysis Using SPSS for Windows*; Palgrave Macmillan: New York, NY, USA, 2003.
84. Jex, S.M. *Stress and Job Performance: Theory, Research, and Implications for Managerial Practice*; Sage Publications: Thousand Oaks, CA, USA, 1998.
85. Lee, R.T.; Ashforth, B.E. A meta-analytic examination of the correlates of the three dimensions of job burnout. *J. Appl. Psychol.* **1996**, *81*, 123–133. [[CrossRef](#)]
86. Podsakoff, N.P.; MacKenzie, S.B.; Podsakoff, P.M. Sources of method bias in social science research and recommendations on how to control it. *Annu. Rev. Psychol.* **2012**, *63*, 539–569. [[CrossRef](#)]
87. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [[CrossRef](#)]
88. Schneider, B.; Ehrhart, M.G.; Macey, W.H. Organizational climate and culture. *Annu. Rev. Psychol.* **2013**, *64*, 361–388. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.