MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17*(4), Article 7. https://doi.org/10.5817/CP2023-4-7

Working Conditions and Cybersecurity: Time Pressure, Autonomy and Threat Appraisal Shaping Employees' Security Behavior

Cornelia Gerdenitsch[1], Daniela Wurhofer[2], & Manfred Tscheligi[1,3]

[1] AIT Austrian Institute of Technology GmbH, Vienna, Austria
[2] Ludwig Boltzmann Institute for Digital Health and Prevention, Salzburg, Austria
[3] Department for Artificial Intelligence and Human Interfaces, University of Salzburg, Salzburg, Austria

Abstract

With the increasing importance of cybersecurity in organizations, it becomes crucial that employees behave securely. In the present article, we investigate the interplay of antecedents on this behavior. We conceptualize cybersecurity behavior through the components of compliance and participation and investigate the relationship between security knowledge, threat appraisal (i.e., severity and susceptibility), and working conditions (i.e., time pressure, decision-making autonomy). We conducted an online survey in four public organizations, collecting quantitative cross-sectional data from 214 employees. The survey captured subjective perceptions of the concepts. Findings showed a positive effect of security knowledge on security compliance and security participation. The perception of severity and susceptibility strengthened both effects. Additionally, the presence of time pressure reduced the effect of security knowledge on security compliance, while having decision-making autonomy increased the effect of security knowledge on security participation. Our study demonstrates the interplay between antecedents and highlights the role of working conditions in employees' cybersecurity behavior. Implications for practice in terms of training approaches considering work design are discussed.

Keywords: cybersecurity; security knowledge; threat appraisal; working conditions; time pressure; decision-making autonomy; perceived severity; perceived susceptibility

Editorial Record

First submission received:
April 19, 2022

Revisions received:
April 11, 2023
June 21, 2023

Accepted for publication:
June 30, 2023

Editor in charge:
David Smahel

Introduction

The increased use of digital technology and internet connections in organisations brings with it a potential growth in cyberattacks (Y. Li & Liu, 2021), intensified by remote working (Philip et al., 2023; Statista, 2022). Protecting against cyberattacks requires not only technical countermeasures but also a focus on human behavior (Algarni et al., 2019; Yan et al., 2018). Indeed, human behavior is noted as one of the biggest challenges when it comes to protecting against cyberattacks (Vrhovec et al., 2023). Human behavior that is secure in the sense of cybersecurity at work implies various facets such as adhering to security policies and guidelines (Nishigaki, 2018) or actively watching out for cyber threats (cf. Griffin & Neal, 2000).

The aim of this work is to investigate the interplay of certain variables on employees' perceived behavior regarding cybersecurity. Here we specifically consider working conditions, as these influence behavior at work. More precisely, we question how employees' perception of knowledge, level of time pressure, decision-making autonomy, and threat appraisal affects perceived cybersecurity behavior.

Previous studies have faced criticism for lacking a clear theory-based conceptualization of cybersecure behavior, making it difficult to compare their findings. Thus, within this article, we start with describing our conceptualization of cybersecurity behavior based on the well-acknowledged theoretical model of safety behavior (Griffin & Neal, 2000; Neal & Griffin, 2006; Neal et al., 2000) and the definition of performance at work by Borman and Motowidlo (1993). We propose two separate components of workplace cybersecurity behavior: compliance and participation (Griffin & Neal, 2000; Neal & Griffin, 2006; Neal et al., 2000).

Although a growing body of research has begun to explore factors that predict workplace cybersecurity behavior (Ameen et al., 2021; Anderson & Agarwal, 2010; Donalds & Osei-Bryson, 2020; Gillam & Foster, 2020; McLeod & Dolezel, 2018; Vrhovec et al., 2023), these studies do not consider the interaction between these factors. In addition, peculiarities of the work context in terms of working conditions have been neglected.

The presented study contributes to research on workplace cybersecurity behavior in a two-fold manner. First, existing research about cybersecurity behavior at the workplace has solely focused on investigating antecedents of this behavior. In contrast, within the present study, we investigate the complex interaction between individual and organizational factors (as recommended by Pham et al., 2017). Second, there is limited research that explores the effect of working conditions in the context of cybersecurity behavior (exception are two studies on the role of time pressure: Collins & Hinds, 2021; Trang & Nastjuk, 2021). Thus, this research attempts to pay attention to work-related circumstances by investigating how working conditions might strengthen or mitigate the effects of security knowledge on security compliance and security participation. Therefore, we consider both a demanding (i.e., time pressure) and supportive (i.e., decision-making autonomy) working condition.

This article is structured as follows: within the next section, we present empirical and theoretical work on cybersecurity behavior, based on which we derive our hypotheses. We then describe our methodological approach and present the findings. Finally, we discuss our findings and provide suggestions for future research as well as give practical implications that should guide managers to foster and maintain the security compliance and security participation of their employees.

Workplace Cybersecurity Behavior

The behavior associated with cybersecurity is complex, encompassing multiple facets (Coventry et al., 2020). This complexity is also reflected in previous research that investigates different aspects, such as awareness (L. X. Li et al., 2019), compliance (Safa et al., 2016), or behavior (Coventry et al., 2020; Trang & Nastjuk, 2021), making it challenging to compare studies. Moreover, even when studying the same aspect, the operationalization can differ. For instance, studies can measure the actual behavior or the intention to show the behavior, they can use self-assessments or external assessments, or focus on general behavior or specifics, such as password use. In addition, there are different types of attacks such as ransomware, malware, or phishing that entail different behaviors and responses from employees (Pyke et al., 2022). To systemize this complexity, frameworks can be helpful. Thus, Guo (2013) proposed a framework for conceptualizing cybersecurity behavior four broad categories: security-assurance behavior, security-compliant behavior, security risk-taking behavior, and security-damaging behavior. To date, several studies have focused on security-compliant behavior (Anwar et al., 2017; Trang & Nastjuk, 2021; Safa et al., 2016) or the intention to engage in that behavior (Blythe & Coventry, 2018), but fewer studies have explored other facets of cybersecurity behavior. Thus, in addition to the need for a clear conceptualization of the researched behavior there is also a lack of research on cybersecurity behavior beyond compliance.

To ensure clear conceptualization of cybersecurity behavior based on established theories, we adopt the model of safety behavior at work by Griffin and Neal (2000) as the basis for our work. This model is widely acknowledged in researching workplace safety behavior and is applicable to security behavior due to key parallels between the two. Organizational and technical arrangements alone do not prevent accidents and incidents completely, and safety and security can only be guaranteed if employees contribute. For this purpose, organizations define policies and procedures and expect employees to adhere to them. In addition, employees can contribute actively to ensure safe and secure behavior. In line with that argumentation and drawing on the definition of individual performance by Borman and Motowidlo (1993), Griffin and Neal (2000) propose two components of safety behavior in the

workplace, which we have adapted here to cybersecurity behavior. *Security compliance* comprises the core activities that employees should carry out to maintain security, such as adhering to security guidelines and procedures defined by the organization. *Security participation*, on the other hand, describes the active engagement of workers in voluntary security activities, such as participating in meetings about security, which helps to develop an organizational environment that supports security. Our conceptualization can be classified into the categories of security-compliant behavior (i.e., security compliance) and security-assurance behavior (i.e., security participation), as formulated by Guo (2013).

Previous studies have examined various antecedents of cybersecurity behavior, such as knowledge and skills (Alnajim & Munro, 2009; Dodge et al., 2012), or personal characteristics (Donalds & Osei-Bryson, 2020). However, less research has focused on how these antecedents interact with each other, and how aspects of the specific context contribute to employees' cybersecurity behavior. To gain a deeper understanding of cybersecurity behavior in the workplace, it is crucial to comprehend the dynamics between these antecedents within the context of the working environment. Therefore, the impact of working conditions must be taken into account. The present study aims to fill this gap by investigating the interplay between antecedents and their effects on employees' cybersecurity behavior. Specifically, we aim to answer the research question of how the interplay between employees' perception of knowledge, threat appraisal, and the two working conditions, namely time pressure and autonomy, affect their cybersecurity behavior. The subsequent sections outline the specific hypotheses.

Security Knowledge

Griffin and Neal (2000) describe that, beyond motivation, knowledge is a central antecedent of behavior. In this vein, security knowledge can be interpreted as a precondition of cybersecurity behavior (Alnajim & Munro, 2009; Dodge et al., 2012). Employees can only comply with security policies and actively participate in cybersecurity when they have the related knowledge (L. X. Li et al., 2019). Thus, we expected a positive effect of knowledge about security issues on cybersecure behavior. We distinguished between security compliance and security participation within our hypotheses as follows.

H1a*:* Security knowledge positively influences security compliance.

H1b: Security knowledge positively influences security participation.

Knowledge alone is often insufficient to produce the desired behavior (Ryan, 2009), also demonstrated in a study on occupational security trainings (Reeves et al., 2021). Workman et al. (2008) described this phenomenon by the term 'knowing better, but not doing better'. Thus, this study investigates whether the effect of knowledge on behavior is influenced (enhanced or diminished) by a set of variables including threat appraisal and two central working conditions—one demanding (time pressure) and one that is considered as a job resource (decision-making autonomy).

Security Knowledge and Threat Appraisal

We consider the perception of a threat as one central variable that influences the effect of security knowledge on behavior. Perceived threat comprises severity and susceptibility, severity being the extent to which individuals perceive that the negative consequences of a threat are severe, and susceptibility describing the subjective likelihood of a threat that affects them. Only when both aspects are present a threat is perceived (Liang & Xue, 2009). Threat appraisal has been studied in the context of security both theoretically (Liang & Xue, 2009) and empirically, whereas empirical studies yield mixed findings in terms of its effect on intention and behavior (e.g., positive effect: Ifinedo, 2014; no significant effect: Vance et al., 2012).

From research in the health context, it is known that perceived severity and susceptibility increase motivation towards a protective action (Protection Motivation Theory; Rogers, 1975, 1983; meta-analysis by Floyd et al., 2000). Following this line of thought, we argue that the perception of a threat not only influences cybersecurity behavior (as has been shown in previous studies) but may also act as a trigger for security knowledge, resulting in cybersecurity behavior. Thus, we expect that security knowledge in combination with a perceived threat is more likely to result in cybersecurity behavior than if only one factor is present. Hence, we are focusing on employees' subjective perception of security threats, rather than objective situational assessment, because different employees may perceive the same threat with varying degrees of severity and susceptibility (Ng et al., 2009). For

instance, one individual may perceive a threat as very likely or as severe, while another may feel the opposite. We have formulated the following hypotheses:

H2a: Perceived severity moderates the relationship between security knowledge and security compliance such that the effect is strengthened when perceived severity increases.

H2b: Perceived severity moderates the relationship between security knowledge and security participation such that the effect is strengthened when perceived severity increases.

H2c: Perceived susceptibility moderates the relationship between security knowledge and security compliance such that the effect is strengthened when perceived susceptibility increases.

H2d: Perceived susceptibility moderates the relationship between security knowledge and security participation such that the effect is strengthened when perceived susceptibility increases.

Security Knowledge and Workplace Time Pressure

Although studies have already explored cybersecurity behaviors in the work context, few studies have considered the role of working conditions. Working conditions are the aspects of a job that can be either demanding or supportive according to the job demands–resources model (Bakker & Demerouti, 2007; Demerouti et al., 2001). These work characteristics further impact work-related consequences such as motivation (Schaufeli & Bakker, 2004), performance (Bakker et al., 2008) and emotional exhaustion (F. Li et al., 2013). Thus, considering working conditions is essential when understanding cybersecurity behavior at work as they are salient in the working context, influencing the emotions and behavior of the working individual.

Time pressure at work describes situations in which employees cannot address all their work tasks due to a lack of time. Experiencing time constraints is a demand, workers are increasingly posed with (see research on work intensification: Green & McIntosh, 2001; Kubicek et al., 2014. Time pressures stem from the pervasiveness of technology and digital interruptions burdening users in their professional and private life, with influences on cybersecurity behavior (Chowdhury et al., 2019). Also, time pressure influences work-related variables such as well-being at work (Sonnentag, 2001), proactive work behavior (Urbach & Weigelt, 2019), or and work engagement (Baethge et al., 2018).

The need to research time pressure in the context of cybersecurity behavior has been emphasized as it influences non-secure behavior (Chowdhury et al., 2019; Trang & Nastjuk, 2021). For instance, it has been found that under time pressure, individuals do not lock their workstations (Chowdhury et al., 2019), or that employees have lowered compliance intentions regarding information security (Hwang & Cha, 2018), leading to non-compliance behavior (Trang & Nastjuk, 2021). One explanation is that during time pressure users rely on habitual behavior (Collins & Hinds, 2021). In line with that we expect that employees that experience high time pressure, will not be able to invest their limited resources to transfer or apply their knowledge about security to their actual security behavior (cf. Chowdhury et al., 2019). Accordingly, the effect of security knowledge on security behavior is diminished for people experiencing higher time pressure, compared to those with lower time pressure. We anticipated this effect for both components of cybersecurity behavior (security compliance and security participation), leading to the following hypotheses.

H3a: Time pressure moderates the relationship between security knowledge and security compliance such that the effect is diminished when time pressure increases.

H3b: Time pressure moderates the relationship between security knowledge and security participation such that the effect is diminished when time pressure increases.

Security Knowledge and Workplace Decision-Making Autonomy

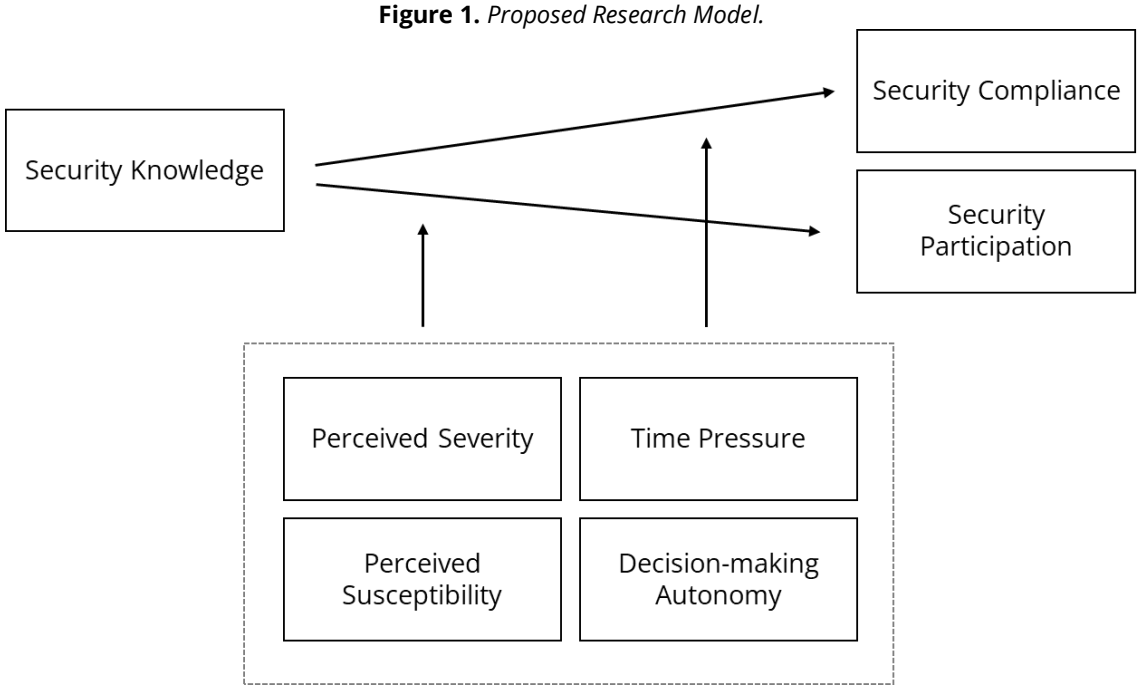
Autonomy is one of the most central job resources and takes several forms in the workplace (De Spiegelaere et al., 2016). One of these is decision-making autonomy, which describes whether workers have the autonomy in their work to make decisions on their own (Morgeson & Humphrey, 2006). A similar construct is work locus of control (i.e., the control workers have over their roles and activities at work), whereas a positive relation to information security behavior has already been demonstrated (Hadlington et al., 2019). We argue that employees with high decision-making autonomy will show a stronger effect of knowledge on behavior compared to those with low decision-making autonomy. The following hypotheses describe our assumption.

H4a: Decision-making autonomy moderates the relation between security knowledge and security compliance such that the effect is strengthened when decision-making autonomy increases.

H4b: Decision-making autonomy moderates the relation between security knowledge and security participation such that the effect is strengthened when decision-making autonomy increases.

In summary, we conceptualized cybersecurity at the workplace via its components of security compliance and security participation and proposed that this behavior at work is determined by security knowledge. We further argue that this effect is contingent on the appraisal of the threat of a cyber-attack and on the working conditions of time pressure and decision-making autonomy. Figure 1 illustrates our research model.

Figure 1. *Proposed Research Model.*



Methods

Sample and Procedure

To test our hypotheses, we prepared an online survey (using LimeSurvey; www.limesurvey.org) to assess the employees' perceptions regarding the study variables. We collected data from employees from four municipalities from three countries (Spain, Portugal and Italy), who participated in an international research project aimed at increasing the resilience of municipalities against cyberattacks (https://cordis.europa.eu/project/id/740712). Data collection took place from October–November 2017. The translation of the survey was organized by one contact persons of each organization. The link to the survey was disseminated by each organization with an introduction stating that the survey aimed to capture experiences regarding workplace cybersecurity as well as individual attitudes and organizational factors. After providing the participants with an explanation of the study and a contact where they can discuss open questions, we asked them if they comprehended the information (yes/no). Subsequently, we sought their consent to participate (yes/no). Only if they answered both questions positively, they could participate in the study. We also assured participants that their identities remain anonymous.

The sample consisted of 214 employees, which is suitable for detecting effects with a medium effect size ($f2$ = 0.15, alpha = .05, power = 0.95; Faul et al., 2009). The mean age of participants was 48.67 years (SD = 9.04), with 59.4% female participants. On average, participants were working 35 hours per week (SD = 9.66) and had worked in their organization for approximately 17.86 years (SD = 10.54).

Measures

The questionnaire comprised 20 items to measure seven study variables. Items to measure security knowledge, compliance, participation, and threat appraisal were adapted from existing scales and items measuring time pressure and autonomy are from existing validated scales. All items were created in English (see Appendix for a

complete list), then translated into the respective languages and provided to the participants in their own language. The following paragraphs describe in detail how each of the study variables was measured.

Security knowledge was measured using three self-developed items assessed on a five-point rating scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). Cronbach's alpha was .91.

Threat appraisal was assessed with four items adapted from Arachchilage and Love (2013) to fit the topic of cybersecurity. We measured perceived susceptibility and perceived severity with two items each. All items were answered on a 5-point rating scale from 1 (*strongly disagree*) to 5 (*strongly agree*). Intercorrelation-coefficients were .85 for perceived severity and .75 for perceived susceptibility.

Time pressure was evaluated using a four-item subscale from the Instrument for Stress-Related Job Analysis (ISTA; Irmer et al., 2019; Semmer et al., 1998). The items were answered using a scale ranging from 1 (*very rarely/never*), 2 (*rarely/approximately once a week*), 3 (*occasionally/approximately once a day*), 4 (*often/several times a day*), to 5 (*very often*). An example item is: *How often are you pressed for time*? Cronbach's alpha was .89.

Decision-making autonomy was captured using a three-item subscale drawn from the Work-Design Questionnaire (Morgeson & Humphrey, 2006). Items were scored on a scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*) and included, for example, *The job allows me to make a lot of decisions on my own*. Cronbach's alpha was .90.

Security compliance and security participation were assessed through items adapted from Neal and Griffin's (2006) and Neal et al., (2000) items regarding the respective safety measures, all measured on a five-point rating scale (1 = *strongly disagree* to 5 = *strongly agree*). Here, Cronbach's alpha was .91 for security compliance and .86 for security participation.

We included age, gender, and tenure as control variables for the analyses.

Analytical Approach

Based on the theoretical considerations, we are assuming effects and therefore formulated and tested alternative hypotheses. To test these, we used regression analyses as an analytical approach. Thereby we controlled for age, gender, and tenure. Following Becker (2005), we excluded the control variables from further analyses when they were not significantly correlated with the dependent variable in the regression model. Tenure was correlated with security participation, but not security compliance. Thus, we conducted all analyses concerning security participation in controlling for tenure. For testing Hypotheses 1a and 1b, we used hierarchical linear regression analysis. To determine moderation (Hypotheses 2–4), we followed the procedure outlined by Hayes (2017) using SPSS PROCESS macro to estimate moderation and mean-centred the product term. Following Dawson (2014), we plotted simple slopes to interpret interaction effects (Aiken & West, 1991).

Results

Descriptive statistics and correlations among the study variables are available in Table 1.

Table 1. *Means (Standard Deviations), Correlations Between the Study Variables, and (Cronbach's Alphas, Intercorrelations-Coefficients*).

	M (SD)	1	2	3	4	5	6	7	8	9	10
1. Age	48.72 (9.03)	—									
2. Gender (1 = *male*, 2 = *female*)	1.41 (0.49)	.08	—								
3. Tenure	17.86 (10.55)	.65**	.06	—							
4. Security knowledge	3.08 (1.12)	−.06	.07	−.03	(.91)						
5. Perceived severity	3.78 (0.98)	.02	.01	−.03	.09	(.85)					
6. Perceived susceptibility	3.48 (0.95)	.03	.05	.06	.03	.55**	(.75)				
7. Time pressure	3.31 (0.99)	−.03	−.02	−.08	−.05	<.01	.11	(.89)			
8. Decision-making autonomy	3.16 (1.31)	−.10	.02	<.01	.22**	−.11	−.04	.09	(.90)		
9. Security compliance	3.67 (0.96)	−.02	.13	−.07	.39**	.03	.12	.10	−.03	(.91)	
10. Security participation	3.10 (1.07)	.01	.10	.11	.42**	.04*	.18*	.04	.09	.53**	(.86)

Note. $N = 214$, $^{*}p < .05$, $^{**}p < .001$, $^{***}p < .001$.

Testing the effect of security knowledge on the two components of cybersecurity behavior (Hypotheses 1a and 1b), we found a positive effect on security compliance, β = .37, $p < .001$; $R^2 = .16$; $F(2, 211) = 21.03$, $p < .001$, and security participation, β = .42, $p < .001$; $R^2 = .19$; $F(2, 211) = 24.90$, $p < .001$. Thus, Hypotheses 1a and 1b were supported.

Further, we tested the interaction effects of threat appraisal (i.e., perceived severity and perceived susceptibility; Hypotheses 2a, 2b, 2c and 2d), time pressure (Hypotheses 3a and 3b) and decision-making autonomy (Hypotheses 4a and 4b) with security knowledge on security compliance and security participation.

Threat appraisal moderated the effect between security knowledge and security compliance. In particular, perceived severity influenced the effect between security knowledge and security compliance ($p = .014$) in a way that the higher the perceived severity, the steeper the slope. The slope was the steepest for employees with very high perceived severity ($B = .59$, $t = 12.50$, $p < .001$), followed by high ($B = .46$, $t = 8.58$, $p < .001$), medium ($B = .34$, $t = 6.17$, $p < .001$), low ($B = .21$, $t = 4.28$, $p = .001$) and very low ($B = .09$, $t = 2.41$, $p = .017$) perceived severity. Security compliance was high when both variables—perceived security knowledge and severity—were high. Interestingly, the effect was reversed in the group of individuals with low perceived security knowledge. In this case, severity decreased compliance. There was no significant interaction effect between security knowledge and perceived susceptibility on security compliance ($p = .661$). Thus, Hypothesis 2a was supported and Hypothesis 2c was rejected.

There was also an interaction effect between security knowledge and threat appraisal on security participation. In particular, we found an interaction effect between security knowledge and perceived severity ($p = .005$) and perceived susceptibility ($p = .007$) on security participation. For perceived severity, the relation between security knowledge and security participation was stronger the higher the perceived severity was. More precisely, the slope was the steepest for employees with very high perceived severity ($B = .71$, $t = 13.79$, $p < .001$), followed by high ($B = .56$, $t = 9.67$, $p < .001$), medium ($B = .41$, $t = 6.95$, $p < .001$), low ($B = .26$, $t = 4.72$, $p < .001$) and very low ($B = .11$, $t = 2.42$, $p = .016$) perceived severity. The interaction pattern was like the one with security compliance; security participation was highest when there was high security knowledge and high severity. When there is low security knowledge, high severity decreased participation. Hypothesis 2b can be supported.

In the case of perceived susceptibility, we found that the slope was the steepest for employees with very high perceived susceptibility ($B = .69$, $t = 14.66$, $p < .001$), followed by high ($B = .54$, $t = 10.01$, $p < .001$), medium ($B = .39$, $t = 6.69$, $p < .001$), low ($B = .24$, $t = 3.96$, $p < .001$) and very low ($B = .09$, $t = 1.49$, $p = .136$) perceived susceptibility. Thereby the effect of knowledge on security participation diminished when there was very low susceptibility. It can be concluded that the effect of security knowledge on security participation was strengthened through perceived susceptibility, meaning that the higher the perceived susceptibility, the stronger the effect on security knowledge and security participation. Based on these results, Hypothesis 2d can be supported. Figure 2, Figure 3 and Figure 4 illustrate all three significant moderating effects.

Figure 2. *Effect of Security Knowledge on Security Compliance Moderated by Perceived Severity (Component of Threat Appraisal).*

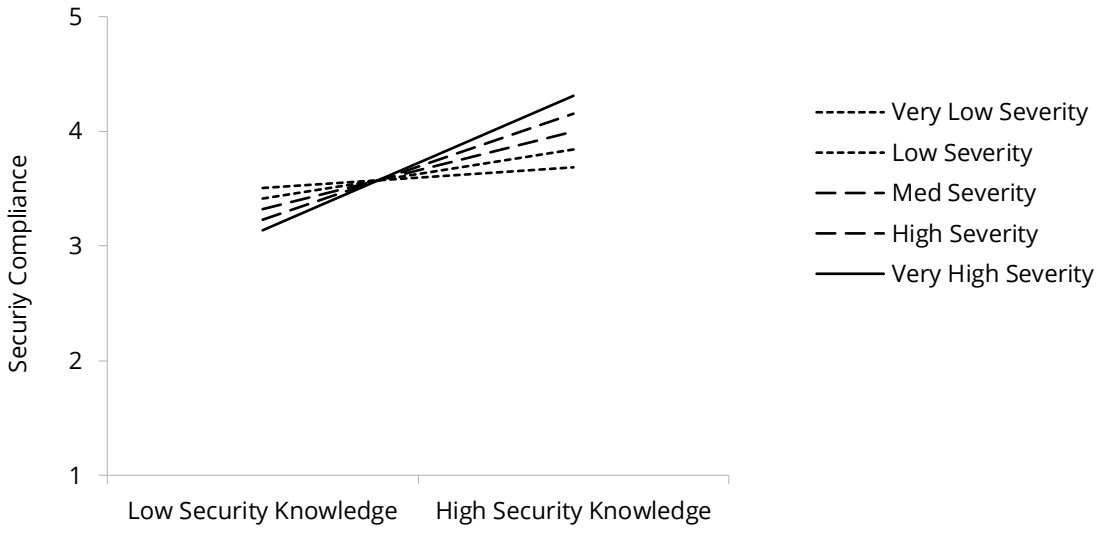


Figure 3. *Effect of Security Knowledge on Security Participation Moderated by Perceived Severity (Component of Threat Appraisal).*

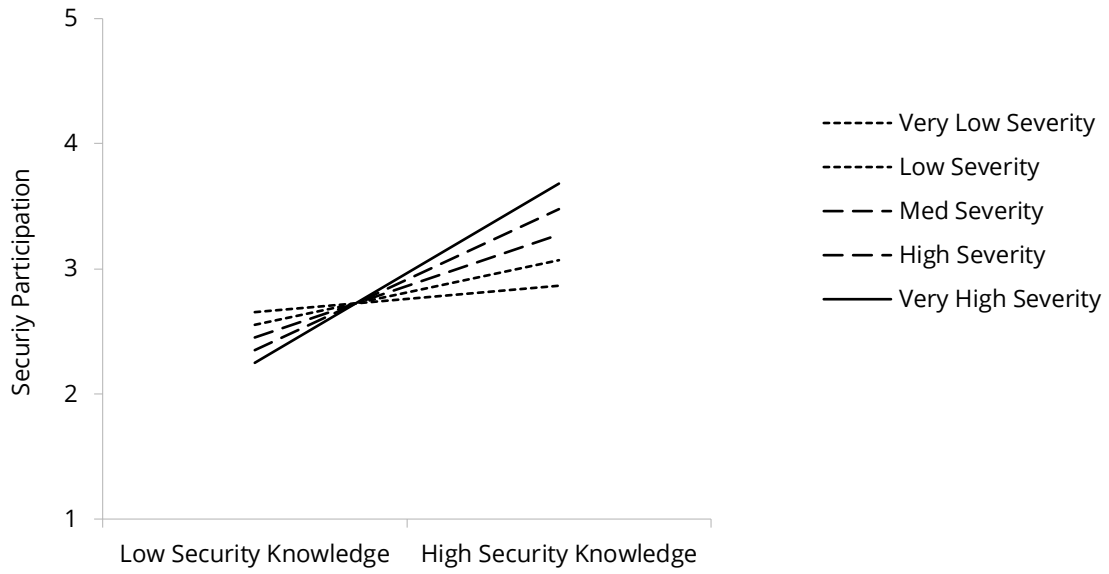
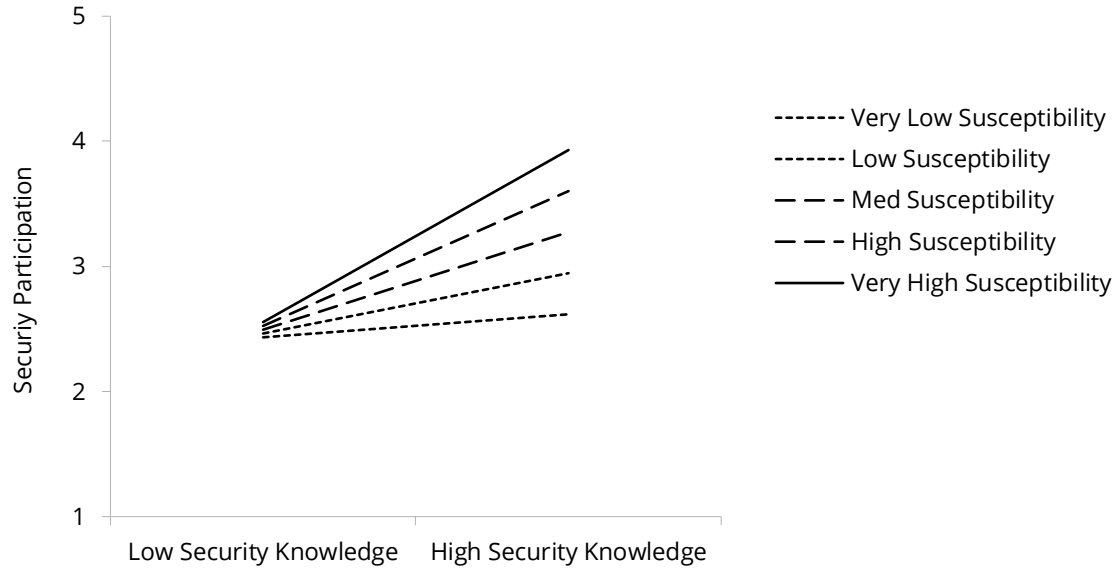
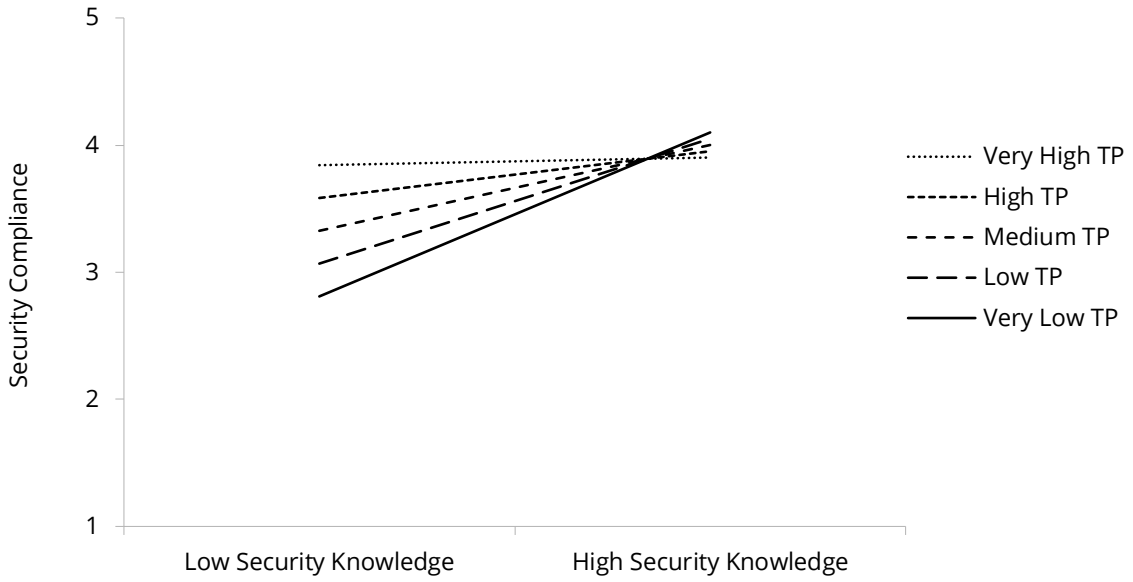


Figure 4. *Effect of Security Knowledge on Security Participation Moderated by Perceived Susceptibility (Component of Threat Appraisal).*



Time pressure moderates the relation between security knowledge and security compliance (p = .006), as seen in Figure 5. The slope was steeper as time pressure decreased, and the slope was steepest for employees with very low time pressure (B = .64, t = 10.60, p < .001), followed by low (B = .49, t = 8.82, p < .001), medium (B = .34, t = 6.27, p < .001), high (B = .18, t = 3.30, p = .001) and very high (B = .03, t = .49, p = .620) time pressure. The effect of security knowledge on security compliance was diminished through time pressure, meaning that in the very high time pressure group, there was no significant effect of security knowledge on security compliance.

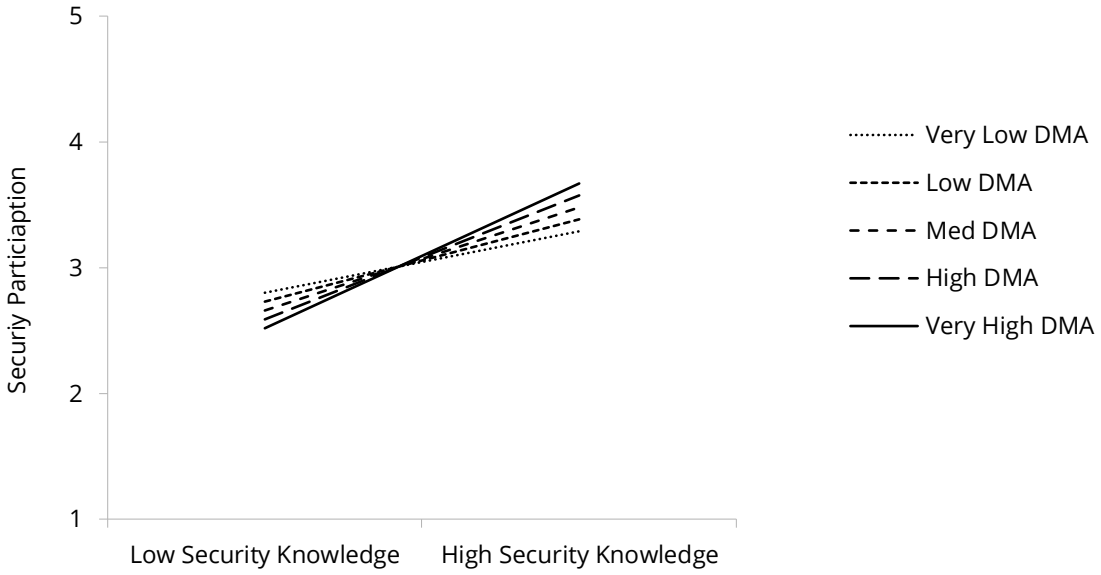
Figure 5. *Effect of Security Knowledge on Security Compliance Moderated by Time Pressure (TP).*



Contrary to our expectation, no moderating effect was found for security participation (p = .160). Thus, Hypothesis 3a was supported, while Hypothesis 3b was rejected.

Decision-making autonomy did not significantly moderate the effect between security knowledge and security compliance (p = .114). However, we did discover an effect of decision-making autonomy on the relation between security knowledge and security participation (p = .066) at a .10 level of significance (see Figure 6). The slope was the highest for the very high group (B = .58, t = 16.00, p < .001), followed by the high (B = .49, t = 8.71, p < .001), medium (B = .41, t = 6.74, p < .001), low (B = .33, t = 6.18, p < .001) and very low (B = .24, t = 10.92, p < .001) groups. The relation between security knowledge on security participation was strengthened by decision-making autonomy. Thus, Hypothesis 4a was rejected and 4b was supported.

Figure 6. *Effect of Security Knowledge and Security Participation Moderated by Decision-Making Autonomy (DMA).*



Discussion

Promoting cybersecure behavior among employees is becoming increasingly important as cyberattacks on businesses increase, also reinforced by the trend toward remote work (Philip et al., 2023). Therefore, it is essential to have a profound understanding of cybersecurity behavior in the working context. In the present study, we conceptualized cybersecurity behavior by adapting the well-recognized model of workplace safety behavior by Griffin and Neal (2000; Neal & Griffin, 2006) to the security context. We investigated the interplay of antecedents on cybersecurity behavior focusing on knowledge and threat appraisal (i.e., perceived severity and perceived susceptibility), time pressures as a demanding, and decision-making autonomy as a supportive working condition. Our study yielded three main findings.

First, we found a positive effect of security knowledge on cybersecurity behavior in terms of security compliance and security participation, supporting previous findings in the specific context of phishing avoidance behavior (Alnajim & Munro, 2009; Dodge et al., 2012). The effect was relatively robust, suggesting that security knowledge has a similar influence on both components of cybersecurity behavior.

Second, we demonstrated that threat appraisal influences the effect of security knowledge on security compliance and security participation. Overall, the higher the threat appraisal (both severity and susceptibility) and knowledge, the higher the security compliance and participation behavior. One explanation may be that threat appraisal may serve as a trigger for transferring security knowledge into the respective behavior. If people perceive that a cyber-attack could happen to them and for that the consequences would be severe, they are triggered to turn their knowledge into behavior.

However, we found different interaction patterns for perceived severity and perceived susceptibility. In the case of susceptibility, it was high susceptibility that was beneficial, while in the case of severity, high severity and high knowledge, as well as low severity and low knowledge, were beneficial for compliance and participation. This effect may be explained by an avoidance reaction of behavior. People who have little knowledge and think that an attack has a gross impact may be afraid or reluctant to deal with the issue. In other words, they do not want to confront it and thus do not enact security participation or security compliance. With these results, we contribute to existing research that has focused on investigating direct effects on threat appraisal on behavior with mixed findings (Ifinedo, 2014; Vance et al., 2012). Our results highlight the need to explore the effects of perceived severity and perceived susceptibility separately. Our findings also show differences between the two considered components of cybersecurity behavior. For security participation, the more active aspect of behavior, both interaction effects are found to be significant, while for security compliance only perceived severity is significant at the .10 level. Thus, our results indicate that threat appraisal is particularly relevant for the more active aspect of cybersecurity behavior.

Finally, this study highlights the influence of characteristics of the working environment (i.e., working conditions) on the relation between knowledge and behavior. We found that the effect of security knowledge on security compliance is diminished by time pressure. There was no positive effect of security knowledge on security compliance for employees reporting very high levels of time pressure. Our results are in line with Hwang and Cha (2018), who found that technostress (security-related stress) lowered employees' compliance intentions regarding information security as well as with Chowdhury et al. (2019), who found effects of time pressure on non-secure cybersecurity behavior. One explanation is that following the security procedures represents a demand on individuals' cognitive resources (D'Arcy et al., 2014) that are not available when there is high time pressure. Findings are also in line with Branley-Bell et al. (2021) who showed that time pressure at work represents a barrier in terms of behavior change towards increased cybersecurity.

On the contrary, we found that decision-making autonomy, strengthened the effect of security knowledge on actively engaging in security behavior. This effect was significant at the .10 level. In contrast to time pressure, decision-making autonomy increases individual resources, helping the individual to engage in proactive behavior. Only when individual employees have the freedom to choose can they actively produce ideas about how to strengthen cybersecurity behavior in the organization. The beneficial effects of autonomy in the context of cybersecurity are in line with the results by Hadlington et al. (2019), who demonstrated that the perception of control within the workplace has beneficial effects on information security awareness.

Contrary to our expectations, we found no empirical support for Hypotheses 3b and 4a. There was no significant interaction effect of time pressure and security knowledge on security participation and no effect of decision-making autonomy and security knowledge on security compliance. It is important to note here that the lack of

confirmation of the proposed alternative hypothesis, which posits a specific effect, does not imply the confirmation of the null hypothesis, which posits no relationship. However, within this study we found effects specifically on security compliance and some on security participation. Our results indicate that job demands limit the effect on cybersecurity behavior, which expresses itself through compliance with rules, while job resources can strengthen the effect on cybersecurity behavior, representing active engagement.

At the theoretical level, we contribute to the research of security-related behavior by introducing the Griffin and Neal framework (2000; Neal & Griffin, 2006) into the discussion on cybersecurity behavior. In this way, we extend previous research that uses the Theory of Planned Behavior (Sommestad et al., 2019), or the Protection Motivation Theory (Hina et al., 2019) by bringing a theory directly from the work context into the scientific discussion. We believe that the complex question of understanding workplace cybersecurity behavior needs different theoretical approaches that provide insights and improve our understanding of this behavior.

Limitations and Future Research

Even though this research offers a strong theoretical contribution by adapting the framework by Griffin and Neal (2000; Neal & Griffin, 2006) to cybersecurity behavior, one of the limitations of the present work is that we tested only one part of the model. Thus, we recommend additional studies to consider security motivation as another antecedent of cybersecurity behavior. Security motivation describes the employee's willingness to invest effort in acting in security-aware ways (adapted from Neal & Griffin, 2006), but it has been studied little in the cybersecurity context. For future studies, we also recommend investigating the effect of organizational factors on cybersecurity behavior. Alshaikh (2020) already explored different initiatives to create cyber security cultures in organisations. In line with that, we recommend paying attention to the concept of the security climate (Chan et al., 2005; Parsons, et al., 2015), which we expect to influence security knowledge and security motivation (cf. Clarke, 2006).

Within this research we chose a method of using a survey instrument to investigate how a set of variables influence the perception of cybersecurity behavior. Since this approach is used frequently, there is a risk that similar studies are repeated without much originality or contribution. Thus, at this point we would like to reflect critically on this approach. We collected cross-sectional data using a self-assessment questionnaire, which has advantages but also limitations. For example, cross-sectional data do not allow us to draw conclusions about the direction of the effect between security knowledge and cybersecurity behavior. In addition, collecting self-reports can raise concerns about common method bias (Podsakoff et al., 2012), which we reduced by using different response formats (Podsakoff et al., 2003). We suggest that future studies will benefit from data triangulation, which involves the use of data from multiple sources to adjust for bias in the different data. This may involve combining self-assessments with external assessments or objective data. For example, knowledge of the organization's security policies can be assessed using objective tests, external assessments from colleagues, and self-assessment. Similarly, security compliance can be assessed using external assessments by colleagues or supervisors, and involvement in security activities can be measured by the number of activities in which someone participates. However, this approach requires appropriate measurement instruments, as they exist for the self-assessment scales. We believe that this lack of standardized methods beyond self-assessments is also a reason why studies stick to the familiar approach. We therefore encourage future research to develop and publish methods and instruments for the purpose of data triangulation.

When investigating cybersecurity behavior, different methodological research approaches can be used, with different levels of abstraction. In the present study, we have chosen an approach that describes cybersecurity behavior on a general level, operationalizing all variables on a general level, which is in accordance with the theoretical model of Neal and Griffin (2000), we used as a framework. We asked participants to self-assess their overall compliance with cybersecurity-related rules and policies without focusing on the specific rules or policies for types of cyberattacks. Yet behavior, participation, and compliance can mean different things in different organizations, and policies vary as well. In addition, not all policies are accurate or up to date, they vary from organization to organization, with some organizations or even teams within organizations being more restrictive than others. So, within this study we assessed rather the representation of what individuals in the organization perceive than actual behavior.

Future research can either focus on specific organizations or explore effects across organizations. To extend the existing research, specific situations in organizational settings can be studied using quantitative diary studies (Ohly et al., 2010) or the qualitative critical incident technique (Butterfield et al., 2005; Flanagan, 1954). This research can for instance investigate if organizational specific procedures and guidelines align with organizational workflows

and thus can be hindering or not. On the other hand, future studies can investigate effects among organizations. In the present study, we sampled employees working in municipalities, which are vulnerable to cyber-attacks due to the sensitive personal data they possess. Similar to our research, we recommend studying organizations from different countries to increase generalizability of the results. Additionally, other studies may want to consider additional variables such as leadership responsibilities, educational level, or corporate position, in addition to the variables of age, gender, and tenure that were examined in this study. When translating the scales, we recommend using a professional translation and in the best case a pretest of the survey instruments.

Given the importance of working conditions in the context of security-related behavior, which we have highlighted in this article, we strongly recommend that studies continue investigating the impact of working conditions. In this study, we examined the moderating effect of time pressure from the source of employees' daily work tasks. Chowdhury et al. (2019) points out that, in addition to this source of time pressure, time pressure can also arise from security-related requirements (see also the construct of security-related stress; D'Arcy et al., 2014). For example, logging on to a computer with additional encryption (e.g., security cue verification) increases the workload and consequently time pressure. Further research that examines time pressure in the context of security-related behavior may explore time pressure from primary working tasks as well as from security-related requirements. Further, we expect that other working conditions influence behavior. For instance, information processing, job complexity (Morgeson & Humphrey, 2006), or task significance (i.e., the degree to which a job influences others; Hackman & Oldham, 1975) could be relevant here.

Implications for Practice

In order to enabling cybersecurity in organizations actions at multiple levels, including the individual, organizational, and societal one are required. At the societal level, Bruijn and Janssen (2017) describe evidence-based framing strategies to increase societal and political awareness of cybersecurity, emphasizing, for example, that cybersecurity should be associated with values other than just security. On an organizational level security training is a prevalent practice that can take the form of either traditional methods or serious games (Švábenský et al., 2018). However, security trainings have its limitations, as it only produces limited changes in behavior (Reeves et al., 2021). Taking up the implications formulated by Gratian et al. (2018) and Torten et al., (2018), who suggest tailoring security training to characteristics of individuals, we formulate two extensions. First, as our study highlights the role of threat appraisal, we suggest training employees in a way that they can better assess the severity and susceptibility. In this vein, organizations can directly respond to the tendency to underestimate the probability of security breaches (de Bruijn & Janssen, 2017; Herath & Rao, 2009). Second, the various facets of security-related behavior have to be considered, as we demonstrated that these can be influenced differently. Third, the study highlights that transferring knowledge into behavior can be hindered by time pressure but be facilitated by giving employees autonomy. This should be considered when designing tailored training. One example would be simulating time pressure. In line with Collins and Hinds (2021), we argue that behavior should be trained to form a habit so that the desired behavior can be exhibited under time pressure.

Conclusion

Gaining an understanding of the (dynamics of the) variables that contribute to cybersecurity behavior is of importance not only for research but also for practitioners to react properly to unsecure behavior. Within this article, we highlight interaction effects between individual and work-related factors on components of cybersecurity behavior. Our findings show that the positive effect of knowledge about security policies and guidelines on cybersecurity behavior can be strengthened by threat appraisal and decision-making autonomy, but it is hampered by time pressure. In this vein, this research has contributed to an understanding of cybersecurity behavior in the workplace, highlighting the role of threat appraisal and working conditions.

Conflict of Interest

The authors have no conflicts of interest to declare.

Authors' Contribution

Cornelia Gerdenitsch: conceptualization, formal analysis, writing – original draft, writing – review & editing. **Daniela Wurhofer:** data curation, methodology, project administration, writing – review & editing. **Manfred Tscheligi:** writing – review & editing.

Acknowledgement

This work was supported by the Compact Project funded under H2020-DS-2016-2017 with the Grant No. 740712.

References

Aiken, L. S., & West, S. G. (1991). *Multiple regression: Testing and interpreting interactions.* Sage.

Algarni, M., Almesalm, S., & Syed, M. (2019). Towards enhanced comprehension of human errors in cybersecurity attacks. In Boring, R. (Eds), *AHFE 2018: Advances in Human Error, Reliability, Resilience, and Performance* (pp. 163–175). Springer. https://doi.org/10.1007/978-3-319-94391-6_16

Alnajim, A., & Munro, M. (2009). Effects of technical abilities and phishing knowledge on phishing websites detection. In *Proceedings of the IASTED International Conference on Software Engineering* (pp. 120–125). ACTA Press. https://www.actapress.com/Abstract.aspx?paperId=34640

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security,* 98, Article 102003. https://doi.org/10.1016/j.cose.2020.102003

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the gen-mobile workforce. *Computers in Human Behavior, 114,* Article 106531. https://doi.org/10.1016/j.chb.2020.106531

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714. https://doi.org/10.1016/j.chb.2012.12.018

Baethge, A., Vahle-Hinz, T., Schulte-Braucks, J., & van Dick, R. (2018). A matter of time? Challenging and hindering effects of time pressure on work engagement. *Work & Stress, 32*(3), 228–247. https://doi.org/10.1080/02678373.2017.1415998

Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. *Journal of Managerial Psychology*, *22*(3), 309–328. https://doi.org/10.1108/02683940710733115

Bakker, A. B., Van Emmerik, H., & Van Riet, P. (2008). How job demands, resources, and burnout predict objective performance: A constructive replication. *Anxiety, Stress & Coping*, *21*(3), 309–324. https://doi.org/10.1080/10615800801958637

Becker, T. E. (2005). Potential problems in the statistical control of variables in organizational research: A qualitative analysis with recommendations. *Organizational Research Methods*, *8*(3), 274–289. https://doi.org/10.1177/1094428105278021

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Borman, W. C., & Motowidlo, S. M. (1993). Expanding the criterion domain to include elements of contextual performance. In N. Schmitt and W. C. Borman (Eds.), *Personnel selection in organizations* (pp. 71–98). Jossey-Bass.

Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting cybersecurity culture change in healthcare. In *PETRA 2021: The 14th PErvasive Technologies Related to Assistive Environments Conference* (pp. 544–549). ACM. https://doi.org/10.1145/3453892.3461622

Butterfield, L. D., Borgen, W. A., Amundson, N. E., & Maglio, A.-S. T. (2005). Fifty years of the critical incident technique: 1954–2004 and beyond. *Qualitative Research, 5*(4), 475–497. https://doi.org/10.1177/1468794105056924

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18–41. https://doi.org/10.1080/15536548.2005.10855772

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology, 38*(12), 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769

Clarke, S. (2006). The relationship between safety climate and safety performance: A meta-analytic review. *Journal of Occupational Health Psychology*, *11*(4), 315–327. https://doi.org/10.1037/1076-8998.11.4.315

Collins, E. I. M., & Hinds, J. (2021). Exploring workers' subjective experiences of habit formation in cybersecurity: A qualitative survey. *Cyberpsychology, Behavior and Social Networking, 24*(9), 599–604. https://doi.org/10.1089/cyber.2020.0631

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *International Conference on Human-Computer Interaction* (pp. 105–122). Springer.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Dawson, J. F. (2014). Moderation in management research: What, why, when, and how. *Journal of Business and Psychology*, *29*(1), 1–19. https://doi.org/10.1007/s10869-013-9308-7

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

De Spiegelaere, S., Van Gyes, G., & Van Hootegem, G. (2016). Not all autonomy is the same. Different dimensions of job autonomy and their relation to work engagement & innovative work behavior. *Human Factors and Ergonomics in Manufacturing & Service Industries, 26*(4), 515–527. https://doi.org/10.1002/hfm.20666

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology, 86*(3), 499–512. https://doi.org/10.1037/0021-9010.86.3.499

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical benefits of training to phishing susceptibility. In *IFIP International Information Security Conference* (pp. 457–464). Springer.

Donalds, C., Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, Article 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327–358. https://doi.org/10.1037/h0061470

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, 108, Article 106319. https://doi.org/10.1016/j.chb.2020.106319

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Green, F., & McIntosh, S. (2001). The intensification of work in Europe. *Labour Economics*, *8*(2), 291–308. https://doi.org/10.1016/S0927-5371(01)00027-6

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational Health Psychology*, *5*(3), 347–358. https://doi.org/10.1037/1076-8998.5.3.347

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242–251. https://doi.org/10.1016/j.cose.2012.10.003

Hackman, J. R., & Oldham, G. R. (1975). Development of the Job Diagnostic Survey. *Journal of Applied Psychology*, *60*(2), 159–170. https://doi.org/10.1037/h0076546

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. https://doi.org/10.1016/j.cose.2018.10.006

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). Guilford Press.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security, 87*, Article 101594. https://doi.org/10.1016/j.cose.2019.101594

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51*(1)*,* 69–79. https://doi.org/10.1016/j.im.2013.10.001

Irmer, J. P., Kern, M., Schermelleh-Engel, K., Semmer, N. K., & Zapf, D. (2019). The Instrument for Stress-Oriented Task Analysis (ISTA): A meta-analysis. *Zeitschrift für Arbeits- und Organisationspsychologie*, *63*(4), 217–237. https://doi.org/10.1026/0932-4089/a000312

Kubicek, B., Korunka, C., Paškvan, M., Prem, R., & Gerdenitsch, C. (2014). Changing working conditions at the onset of the twenty-first century: Facts from international datasets. In C. Korunka & P. Hoonakker, *The impact of ICT on quality of working life* (pp. 25–41). Springer Science + Business Media. https://doi.org/10.1007/978-94-017-8854-0_3

Li, F., Jiang, L., Yao, X., & Li, Y. (2013). Job demands, job resources and safety outcomes: The roles of emotional exhaustion and safety compliance. *Accident Analysis & Prevention*, *51*, 243–251. https://doi.org/10.1016/j.aap.2012.11.029

Li, L. X., 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. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90. https://doi.org/10.2307/20650279

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

Morgeson, F. P., & Humphrey, S. E. (2006). The Work Design Questionnaire (WDQ): Developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of Applied Psychology*, *91*(6), 1321–1339. https://doi.org/10.1037/0021-9010.91.6.1321

Neal, A. C., Griffin, M., & Hart, P. M. (2000). The impact of organizational climate on safety climate and individual behavior. *Safety Science, 34*(1–3), 99–109. https://doi.org/10.1016/s0925-7535(00)00008-4

Neal, A., & Griffin, M. A. (2006). A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels. *Journal of Applied Psychology*, *91*(4), 946–953. https://doi.org/10.1037/0021-9010.91.4.946

Neal, A., Griffin, M. A., & Hart, P. M. (2000). The impact of organizational climate on safety climate and individual behavior. *Safety Science*, *34*(1–3), 99–109. https://doi.org/10.1016/S0925-7535(00)00008-4

Ng, B.-Y., Kankanhalli, A., & Xu, C. Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4)*,* 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nishigaki, M. (2018). Humanics information security. *Concurrency and Computation: Practice and Experience*, *30*(2), Article e4274. https://doi.org/10.1002/cpe.4274

Ohly, S., Sonnentag, S., Niessen, C., & Zapf, D. (2010). Diary studies in organizational research: An introduction and some practical recommendations. *Journal of Personnel Psychology, 9*(2), 79–93. https://doi.org/10.1027/1866-5888/a000009

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129. https://doi.org/10.1177/1555343415575152

Pham, H., Brennan, L., & Richardson, J. (2017). Review of behavioural theories in security compliance and research challenge. In *Proceedings of the Informing Science and Information Technology Education Conference, Vietnam* (pp. 65–76). Informing Science Institute. https://doi.org/10.28945/3722

Philip, S. J., Luu, J. T., & Carte, T. (2023). There's no place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior, 139,* Article 107551. https://doi.org/10.1016/j.chb.2022.107551

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, R. (2022). Predicting individual differences to cyber-attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15*(4), Article 9. https://doi.org/10.5817/CP2021-4-9

Reeves, A., Calic, D., & Delfabbro, P. (2021). Get a red-hot poker and open up my eyes, it's so boring: Employee perceptions of cybersecurity training. *Computers & Security, 106*, Article 102281. https://doi.org/10.1016/j.cose.2021.102281

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In B. L. Cacioppo & L. L. Petty (Eds.), *Social psychophysiology: A source book* (pp. 153–176). Guildford Press.

Ryan, P. (2009). Integrated theory of health behavior change: Background and intervention development. *Clinical Nurse Specialist*, *23*(3), 161–170. https://doi.org/10.1097/NUR.0b013e3181a42373

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Schaufeli, W. B., & Bakker, A. B. (2004). Job demands, job resources, and their relationship with burnout and engagement: A multi-sample study. *Journal of Organizational Behavior, 25*(3), 293–315. https://doi.org/10.1002/job.248

Semmer, N. K., Zapf, D., & Dunckel, H. (1998). *Instrument zur streßbezogenen Tätigkeitsanalyse ISTA [Instrument for stress related job analysis ISTA]*. Verlag der Fachvereine Hochschulverlag. https://www.uni-frankfurt.de/45673143/Stressbezogene_Arbeitsanalyse_mit_ISTA

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems, 59*(4)*,* 344–353. https://doi.org/10.1080/08874417.2017.1368421

Sonnentag, S. (2001). Work, recovery activities, and individual well-being: A diary study. *Journal of Occupational Health Psychology, 6*(3)*,* 196–210. https://doi.org/10.1037/1076-8998.6.3.196

Statista (2022, May 5). *Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working worldwide in 2021, by country*. https://www.statista.com/statistics/1259560/ciso-organization-cyberattacks-remote-work-by-country/

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018). Enhancing cybersecurity skills by creating serious games. In *ITiCSE 2018: Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp. 194–199). ACM. https://doi.org/10.1145/3197091.3197123

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79,* 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security, 104,* Article 102222. https://doi.org/10.1016/j.cose.2021.102222

Urbach, T., & Weigelt, O. (2019). Time pressure and proactive work behaviour: A week-level study on intraindividual fluctuations and reciprocal relationships. *Journal of Occupational and Organizational Psychology, 92*(4), 931–952. https://doi.org/10.1111/joop.12269

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security, 125*, Article 103038. https://doi.org/10.1016/j.cose.2022.103038

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Appendix

Table A1. *List of Questions Separately for the Study Variables.*

Security knowledge[*]
I know about the cybersecurity risks in my workplace.
I know how to work cybersecurity aware.
I know about how to avoid cybersecurity risks in my workplace.

Threat appraisal: Perceived susceptibility[*]
It is extremely likely that my computer will be infected by a (cyber)security-attack in the future.
My chances of getting a cyber-attack are great.

Threat appraisal: Perceived severity[*]
A cyber-attack would steal my personal information from my computer without my knowledge.
A cyber-attack would invade my privacy.

Time Pressure[**]
The questions are available in English and German under the supplemental material of the article by Irmer et al. (2019; https://doi.org/10.1026/0932-4089/a000312).

Decision-making autonomy[*]
The questions are available in different languages on the homepage describing the work design questionnaire (WDQ): http://www.morgeson.com/wdq.html

Security compliance[*]
I hold in mind the cybersecurity guidelines when I do my job.
I use the correct cybersecurity procedures for carrying out my job.
I ensure the highest levels of cybersecurity when I carry out my job.

Security participation[*]
I promote the cybersecurity guidelines within the organization.
I put in extra effort to improve cybersecurity of the workplace.
I voluntarily carry out tasks or activities that help to improve workplace cybersecurity.

Note: [*]Likert scale from 1 (*strongly disagree*) to 5 (*strongly agree*); [**]Likert scale from 1 (*very rarely/never*), 2 (*rarely/approximately once a week*), 3 (*occasionally/approximately once a day*), 4 (*often/several times a day*), to 5 (*very often*).

About Authors

Cornelia Gerdenitsch works as a Post-Doc Researcher at the AIT Austrian Institute of Technology. She obtained her PhD in the field of occupational and work psychology, focusing on digital work and its impact on workers' behavior and emotions. Cornelia's research interests include the design of digital workplaces and tools, such as mixed reality applications, in both office and industry sectors. She also investigates the effects of digital workplaces and the changes related to workers.

https://orcid.org/0000-0003-1502-8543

Daniela Wurhofer works as a Post-Doc Researcher at the Ludwig Boltzmann Institute for Digital Health and Prevention. Studying Psychology and Applied Computer Science, she did her PhD in the field of Human-Computer Interaction, with a focus on temporal transitions of user experience, i.e., investigating changes of users' experiences over time. Next to user experience, Daniela's interests include user-centered development of digital health interventions, Shared Decision Making with digital health applications, as well as acceptance of mobile and automated technologies.

https://orcid.org/0000-0001-8476-6051

Manfred Tscheligi is a Professor at the University of Salzburg, where he serves as the Head of the Department for Artificial Intelligence and Human Interfaces. Additionally, he leads the Center for Technology Experience at the AIT Austrian Institute of Technology in Vienna. His work primarily focuses on harnessing the interdisciplinary synergy of various fields to enhance the interaction between humans and systems.

https://orcid.org/0000-0001-6056-7285

✉ **Correspondence to**
Cornelia Gerdenitsch, AIT Austrian Institute of Technology, Gieffinggasse 4, 1210 Vienna, Austria,
cornelia.gerdenitsch@ait.ac.at