How to Mitigate Security-Related Stress: The Role of Psychological Capital

Muriel Frank
Goethe University Frankfurt
frank@wiwi.uni-frankfurt.de

Vanessa Kohn
Goethe University Frankfurt
kohn@its.uni-frankfurt.de

Abstract

In an organizational context, individuals are prone to feel stressed by overwhelming and complicated security requirements, which can result in noncompliance with security policies and guidelines. While previous research has mainly focused on identifying distinct dimensions of security-related stress (SRS) and their behavioral impact, this paper is the first to examine factors for mitigating SRS. A study with 150 participants reveals that psychological capital (PsyCap) – here comprising of domain-specific self-efficacy and resilience – may work as such a means as it significantly reduces perceived SRS. However, the positive effect of PsyCap diminishes when becoming a victim of cybercriminals. Said differently: victims displaying high or low PsyCap tend to feel more stress compared to non-victims. Our findings imply that organizations should invest in measures that help their employees to develop positive mental capabilities before experiencing an information security incident.

1. Introduction

Over the last decade, both the quantity and severity of information security breaches have increased tremendously [34]. Cybercriminals continuously find new ways to compromise, steal, or manipulate sensitive data confronting organizations with massive financial losses [54]. In many cases, such attacks are successful because they take advantage of the weakest link, the human factor [24]. To counteract these security risks, organizations have started to employ different kinds of measures, such as specific security guidelines and policies [1]. These measures are designed to provide employees with the necessary knowledge to reduce the probability of becoming victims of malicious hackers.

Concurrently, employees often perceive those measures as overwhelming and difficult to understand [17]. Besides, seeing their information security behavior to be monitored and, consequently, their privacy invaded also puts stress on individuals [1]. Therefore, it is not surprising that security-related stressors negatively relate to information security compliance intentions [1, 17].

In order to achieve secure information systems, it seems necessary to help individuals to face security-related stress and still evince sound information security behavior. So far, researchers have only focused on dimensions or the outcome of security-related stress (SRS) [1, 17], leaving room for investigations on potential stress mitigators.

We argue that employees need to develop a positive mental state, also known as psychological capital (PsyCap), to counter the harmful effects of security-related stress. PsyCap is positively related to desirable employee attitudes, behaviors, and performance measures while it decreases undesirable attitudes such as cynicism, turnover intentions, and deviant employee behavior [3]. Yet, the impact of PsyCap in information security remains unexplored, though we see promising research findings concerning the two PsyCap subdimensions resilience and self-efficacy. For instance, Bulgurcu et al. [8] confirm a significantly positive relationship between self-efficacy and compliance with security policies. McCormac et al. [45] recently explored how job stress relates to resilience and information security awareness. They find that resilience effectively mediates the relationship between job stress and awareness, meaning that even when faced with lots of stress at work, resilient employees still report higher levels of security awareness. By investigating the role of PsyCap in mitigating security-related stressors, this study aims at closing this research gap. Accordingly, the main research question is:

Does psychological capital work as a means to mitigate employees' information security stress?

To the best of our knowledge, we are the first to test whether PsyCap works as a mitigator with regard to SRS. By doing so, we can gain essential insights into employees' security behavior and understand what factors contribute to the extent people

URI: https://hdl.handle.net/10125/71167
978-0-9981331-4-0

experience security-related stress. Our findings are of high practical relevance as managers in charge learn how individual characteristics and mental capabilities affect their employees' security-related stress levels and, consequently, may adjust their strategies.

The paper is organized as follows. First, we describe the study's primary constructs, namely PsyCap and security-related stress. The next section entails information on the research method as well as the data collection procedure, sample characteristics, as well as the applied measures. This is followed by the analysis. Afterward, we discuss theoretical as well as practical implications and finalize the section by looking at future research endeavors.

2. Theoretical context

The purpose of this study is to gain a better understanding of whether a positive psychological state can reduce the unwanted outcomes of security-related stress. In the following, we give a brief overview of the constructs our research model consists of, including current research findings. The final subsection presents the model (see Figure 1) as well as our hypotheses.

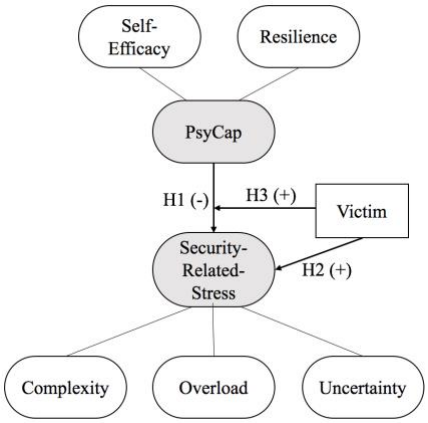

Figure 1. Research model

2.1. Psychological capital

The concept of psychological capital emerged in the late 1990s as part of the positive psychology movement [9], which aims at focusing on strengths, motives, and capacities of human beings rather than their errors and weaknesses [11, 58]. It comprises, amongst others, the two components self-efficacy and resilience [39], which are necessary to successfully reach a goal [11] and already played a significant role when examined as individual components in information security [8, 45].

Self-efficacy draws on Social Cognitive Theory [16] and is defined as "one's confidence in his or her ability to mobilize the motivation, cognitive resources, and courses of action necessary to execute a specific course of action within a given context" [40:158]. It is essential to distinguish self-efficacy from the general term confidence. Confidence describes the strength of a belief without specifying to what the certainty refers. For instance, one can be highly confident to fail at a task. In contrast, self-efficacy refers to a person's belief in their capability to follow a course of action leading to the attainment of given objectives [5]. While confidence is a general characteristic of a person, self-efficacy is a domain-specific construct containing both the affirmation of one's ability and the strength of belief [48]. Drawing on the difference between the terms, confidence rather works as a dependent variable in the information security context, whereas self-efficacy can be characterized as an independent variable that may be targeted for interventions and utilized as an antecedent of change [16].

A significant number of studies proves the positive relationship of self-efficacy on behavioral outcomes in different settings [62]. People who are confident about being able to cope with any situation tend to carry on higher risks [4]. The concept of self-efficacy has also been transferred to the field of information security. Several studies reveal the positive relationship self-efficacy has on information security policy compliance [8, 27, 31, 32, 60] and information security knowledge sharing intentions [63]. The more individuals believe in having the skills and capabilities to follow the information security rules or to have the necessary security knowledge, the higher their intention to comply or share.

In the literature devoted to psychology, **resilience** is seen as a "phenomenon of competence despite adversity" [42:554] and "good outcomes in spite of serious threats to adaptation or development" [44:228]. These definitions suggest that individuals are capable of adapting well even under challenging life conditions such as adversity, trauma, or stress [2, 67]. Findings show that resilience is also associated with self-efficacy [44]. In an organizational context, resilience describes the ability of employees to use existing resources to overcome challenging situations and to bounce back in the workplace [49]. It is characterized by three underlying factors: adaptability, networking, and learning [35]. Research therefore suggests that resilience can be specifically developed and promoted through organizational

measures [65]. The concept of resilience has only recently found its way into the field of information security. Ole Johnsen [50], for instance, explored how to increase resilience to mitigate unwanted intrusion into networks. More recently, [34] links employees' resilience to improved information security behavior in terms of proactive awareness, password generation, as well as device securement and updating. Additionally, [45] analyze how job stress connects to resilience and security awareness. The authors find that resilient individuals have more security knowledge and are more aware of potential security issues. The same applies to those who reported being less stressed at work.

2.2. Security-related stress

At least since organizations know about the potential threat of abusive insiders, they require their employees to abide by strict security rules and regulations [55]. For instance, workers are not allowed to share their passwords with colleagues, send sensitive data unencrypted, or read confidential data [66]. However, when being confronted with complex and obscure security practices, most employees feel stressed, which has a negative impact on their intention to comply [1, 36]. Puhakainen and Siponen [56], for instance, demonstrate employees' stressful reactions to such requirements. And Posey et al. [55] find employees who are confronted with constantly changing security environments to be prone to computer abuse.

Early work in the realm of security-related stress also proves that information security requirements may create stress. D'Arcy et al. [17], for instance, transfer the concept of technostress to information security. Drawing on coping theory as well as prior technostress research, they explore the three factors security-related overload, security-related uncertainty, and security-related complexity. They find these stressors to negatively affect an individual's willingness to comply with security policies. Ament and Haag [1] approach the topic from a different perspective. They expect security-related stress to be a multidimensional construct, spanning not only employees' work but also their personal and social environment. With the help of 165 participants, they identify three additional stressors, namely privacy invasion, conflict, and news, which all have a significant impact on information security awareness.

Recent research approaches examine other stress-related antecedents of security policy compliance. Hwang and Chao [30] demonstrate that security-related role stress as well as security-related technostress creators, such as complexity, overload, and uncertainty, decrease one's organizational commitment, which indirectly affects one's compliance with security policies. Building on protection motivation theory, [12] find that stress significantly influences coping strategies and, thus, security policy compliance.

2.3. Hypotheses

Today's organizations often have security requirements, rules, and policies in place, which may have an opposing effect *(*though*)*. Instead of promoting information security, employees often feel overwhelmed and stressed, making them less willing to follow the rules [17]. As highlighted in the previous section, information security researchers have identified several stressors that negatively impact one's compliance intention, including complexity, uncertainty, and overload [1, 17]. Individuals do not have the resources to invest heavily in understanding changing or overwhelming policies.

Previous findings have already confirmed the important relationship of PsyCap with positive organizational outcomes, like job satisfaction [3] and reduced turnover [53]. Directly relevant to the present study, Baron et al. [6] find psychological capital to be a sufficient buffer against stress. Additional findings from McCormac et al. [45] confirm that more resilient people tend to report lower stress levels. As PsyCap reflects how people cope with stressful or disastrous events [39], we assume this positive mental state to play a significant role in the security context as well. Those who feel confident to cope with information security incidents should report significantly lower stress levels. This notion is backed up by findings which show that the concepts of stress and self-efficacy are closely related [69], suggesting that people who feel self-confident are more likely to assess a given situation as rather challenging than threatening [13]. Based on the above evidence, we assume employees with higher psychological capabilities such as self-efficacy and resilience to experience less security-related stress and thus hypothesize:

H1: PsyCap is negatively related to security-related stress.

Research shows that traumatic incidents are often followed by stress [37]. For instance, employees who experienced workplace bullying commonly report a loss of confidence and increased stress levels [64]. Stressors can be classified into four categories: major

life events, catastrophes, daily hassles, and conflict [52]. Major life events are good or bad life changes (e.g., a divorce or a jail term) that require an individual to adjust. Catastrophes encompass natural disasters and wars, whereas daily hassles (e.g., concerns about money or discrimination) add up over time. Crises require individuals to choose between multiple demands, needs, or desires.

Depending on the severity and consequences, being the victim of an information security incident at work can be classified as a daily hassle, conflict, or even a life event – if an employee loses their job and reputation over the incident. To the best of our knowledge, no prior research has analyzed the post-incident stress levels of employees who experienced information security incidents. Based on the above classification and evidence from other contexts, we assume employees who were already once tricked by cybercriminals to perceive higher levels of security-related stress, as they realize their blatant incompetence to behave securely.

H2: Previous exposure to information security incidents is positively related to security-related stress.

To further investigate the relationship between PsyCap and SRS, we focus on interaction effects between both constructs. As stated above, we assume psychological capital and security-related stress to be negatively related. But while we expect a stress-reducing impact of self-efficacy and resilience for all employees, we assume that the strength of this impact differs for those who already experienced information security incidents either in their private or in their professional lives (see Figure 1). Drawing on findings from the psychological sphere [48, 59], we expect former victims of cybercriminals to feel more stressed by complex security requirements compared to individuals with no incident experience and, therefore, less confident about coping with future information security incidents. That may be because employees who already experienced a security incident may realize that they failed to fully understand all security requirements or to act accordingly. In other words: Prior incident experience may work as a stress trigger showing those affected their incompetence to abide by security guidelines. A positive mental state is then less effective. Employees with no incident experience, however, may still be confident to handle security practices and, hence, feel less stressed. Correspondingly, we hypothesize the following:

H3: The relationship between PsyCap and security-related stress is moderated by previous exposure to information security incidents.

3. Methodology

In the ensuing section, we present details on the scale development, the demographic characteristics of the data sample, and the collection procedure. To investigate whether psychological capital relates to security-related stress, we collected data from 150 employees through an online survey and then applied structural equation modeling in Amos 27.

3.1. Scale development & measures

The Psychological Capital Questionnaire (PCQ) is considered to be the standard scale to measure PsyCap in an organizational setting [38]. Its 24 items revolve around the workplace (e.g., “If I should find myself in a jam at work, I could think of many ways to get out of it”), but do not capture security-specific situations. As a result, a more targeted PsyCap scale in the context of information security is needed, which has been recently highlighted by Burns et al. [9], who established a connection between PsyCap in general and all components of protection motivation theory. As no prior research has transferred the concept of PsyCap to the context of information security, we followed the approach of Morgado et al. [47] for item generation. This implied a literature review, expert sessions, and psychometric analysis. We developed items for self-efficacy based on Luthans et al. [39] and Klesel et al. [33]. The resilience items are adapted from the Employee Resilience Scale [34, 49]. For instance, the item “I effectively collaborate with others to handle unexpected challenges at work” was modified to “I effectively collaborate with others to handle unexpected security challenges”. All items were checked by three experts in terms of coherency and comprehensibility.

In order to measure participants’ positive mental capabilities, we asked them to read a short scenario of an information security incident and subsequently evaluate their agreement with the items presented in Table 1. Using scenarios to measure behavior is well established in the field of information security [see i.e. 33]. Based on the contextual information provided, participants tend to answer the questions honestly [22]. Here, participants were asked to imagine that they have accidentally downloaded a virus on their work computer. By specifying the nature and consequences of the security incident and

giving examples for security guidelines, we align participants' answers irrespective of external factors such as the presence of certain security policies in the participants' workplace.

We drew on established items to measure security-related stress [17]. We further asked participants to indicate whether they have previously been a victim of any security incident affecting either their private or professional life.

Table 1. Final PsyCap survey items

	Item
Self-Efficacy	I feel confident that I can adapt to new security requirements.
	I am willing to put in effort to understand new security policies.
	I re-evaluate my security performance and continually improve the way I do my work.
	I make a plan to integrate new regulations in my work routines.
Resilience	I effectively collaborate with others to handle unexpected security challenges.
	I seek assistance when I need specific information security resources.
	I approach managers when I need their support regarding information security.
	I learn from my mistakes and improve the way I follow security guidelines.
	I effectively respond to feedback about my security behavior, even criticism.
	I use this change at work as an opportunity for growth.

With the collected survey data, we first performed an exploratory factor analysis to confirm that all newly developed items load together as psychological capital. In the course of this, the items for hope had to be excluded due to cross-loadings. Afterward, we conducted a confirmatory factor analysis to specify whether to use a first-order or a second-order construct. For optimism, however, we found issues regarding its internal consistency, so we decided to drop it from further analysis. Results suggested proceeding with the better-performing second-order construct of PsyCap, containing the individual components self-efficacy and resilience, which is in line with prior research [9, 39]. The internal consistency of PsyCap is 0.954.

3.2. Sample data

We collected 150 data sets by distributing an online questionnaire over crowdsourcing marketplace Amazon MTurk, which is no longer an exception in scientific research [51]. Data collected via online labor markets are externally and internally valid [7]. We required participants to live in the United States to avoid cultural biases in our sample. To further guarantee high data quality, we controlled for incomplete data sets and low participation times. Besides, the survey included control questions, and we eliminated data sets of participants who failed to give the right answers. In total, 13 data sets had to be removed. The remaining 137 data sets were used for further analysis, such as exploratory and confirmatory factor analysis and structural equation modeling in Amos 27.

The majority of participants are males (62.8 %). The average respondent is 36.0 years old and has a working experience of 13.65 years. Participants spread almost evenly over all industries, with a majority working in Software & IT Services (25.5%) and Retail, Wholesale & Distribution (13.1%). Furthermore, participants reported a relatively high educational level, with more than 52% of them having a Bachelor's degree. The majority of the respondents work in companies with more than 100 employees.

3.3. Analysis

A KMO value of 0.924 and a significant Bartlett spherical value indicate that our data is suitable for factor analysis. Initially, we included all four sub-constructs of PsyCap in our exploratory factor analysis.

All items in the confirmatory factor analysis show loadings above 0.6. Reliability and validity values are well above the recommended thresholds [23], with all three factors having an average variance extracted of 0.8 or more and composite reliability of above 0.9. Following Fornell and Larcker (1981), we also checked discriminant validity and compared the square root of the AVE with the correlations between constructs. All values confirmed validity. Comparing the fit indices against the acceptable thresholds [23], we find the model to have excellent goodness of fit. CFI and TLI amount to 0.972 and 0.929, respectively, SRMR and RMSEA to 0.052 and 0.041.

4. Results

As displayed in Figure 2, the path between PsyCap and security-related stress is significantly negative (-0.256). Hence, the model confirms our expectation that employees with high PsyCap experience less stress when being exposed to complex, overwhelming, and uncertain security requirements (hypothesis 1).

As expected, employees who previously experienced an information security incident displayed significantly higher levels of security-related stress (.277). This finding supports our second hypothesis.

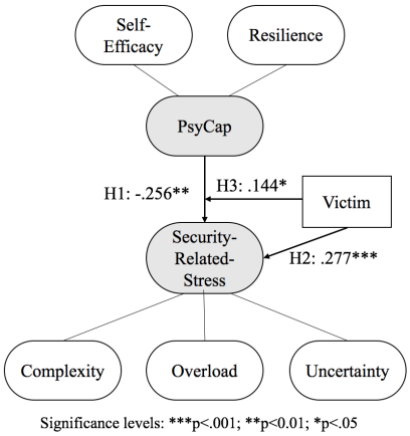

Figure 2. Research results

In line with hypothesis 3, we detect a moderating effect (.144) of previous exposure to security incidents on the relationship between PsyCap and security-related stress. This implies that the negative impact of PsyCap on security-related stress is dampened when an employee has already become the victim of an information security incident. Figure 3 illustrates this interaction effect.

We also find victims to be more stressed compared to employees who have no incident experience (3.420 vs. 2.686). These differences are statistical significant ($Z=-4.217$, $p<0.000$). Furthermore, the latter reported higher PsyCap levels compared to those who already had to deal with a security incident in the past (4.368 vs. 3.996). Again, these group differences are significant ($Z=-2.757$, $p<0.006$).

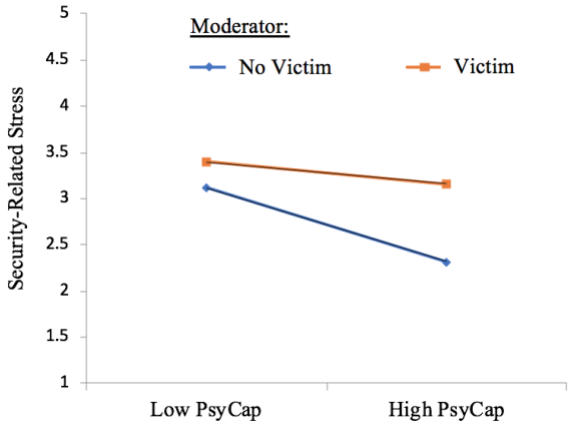

Figure 3. Interaction effect

When controlling for gender, we found no significant effect. However, age has a small positive effect on PsyCap (.174*), indicating that older employees show a slightly higher positive mental state.

5. Discussion

In this paper, we introduced the concept of security-specific PsyCap and demonstrated its impact on security-related stress. In the following section, we will discuss the practical and academic implications of our findings. We conclude by making suggestions for future work while accounting for the limitations of the current study.

5.1. Contributions and implications

To the best of our knowledge, we are the first to develop and validate a scale measuring psychological capital specific to the information security context. By doing so, we contribute to the emerging body of PsyCap research in general [6] as well as to more recent findings with regard to information security [9]. Our PsyCap scale comprises ten items divided into the two components resilience and self-efficacy. Yet, it is noteworthy that these constructs of PsyCap may not be seen as an exclusive taxonomy of what constitutes the determining factors for an employee's security-related stress level. Instead, we suggest them to play an essential role in contributing to a better understanding of whether individuals experience security-related stress and abide by security rules and regulations. As this is the first empirical study to apply our new scale, further validation is needed. Hence, we highly encourage future researchers to draw on our scale when investigating psychological and behavioral influences in the field of information security.

Moreover, we are the first to discover that PsyCap can work as a mitigator on security-related stress, which is a new and important finding. People scoring high on PsyCap are less prone to stress. This finding is in line with previous studies from other disciplines. Baron et al. [6], for instance, confirm that PsyCap leads to improved well-being. Our result underlines the importance of investing in employees' PsyCap to reduce their perceived stress levels. By doing so, the overall compliance with security requirements can increase [1, 36]. In other words: If organizations want their employees to follow security guidelines, they should write them in a clear language and communicate them through high-level managers [60].

Our results also advise managers in charge to focus their efforts on strengthening their employees' PsyCap through targeted training measures [53]. Intervention strategies could encompass including employees in the process of developing security goals and breaking them down into small achievable tasks as well as encouraging employees to perceive security threats as opportunities to protect the organization rather than potential points of failure [9]. PsyCap thus represents a powerful lever for reducing a workforce's security-related stress and thereby improving their compliance with security policies. Prior research has also shown that the compliance behavior of employees positively affects the security behavior of their peers [25]. We therefore assume that employees with high PsyCap are contributing to a higher security level in their organizations not only by being less stressed about security requirements and more careful in following security policies but also by inspiring their colleagues to do the same.

Literature confirms higher levels of stress amongst those who experienced traumatic situations such as being the victim of a crime or going through emotionally intense experiences [52]. We were the first to study the influence of exposure to information security incidents on employees' security-related stress levels. In line with research results from other fields, victims of cybercrime reported significantly higher security-related stress. We advise practitioners to foster a proactive workplace culture in which employees feel safe to make mistakes and share their failures [19]. When promoting proactive communication, organizations can decrease or even prevent their employees from experiencing security-related stress and making mistakes in the future [15, 29, 43]. That is because scholars have already proven a positive relationship between learning from mistakes and resilience [10]. Employees who are able to cope with setbacks better generally also perform better and show greater commitment because they are aware of challenging situations and expect failure [28]. As a result, they will develop a stronger sense of responsibility and a higher intrinsic motivation for dealing with and correcting mistakes [21], which is what we find here. Those scoring high on psychological capital perceived less security-related stress compared to employees with low PsyCap.

Noteworthy is the moderating effect of exposure to information security incidents. If employees had become a victim of cybercriminals, the negative effect of PsyCap on SRS was less strong, meaning that the positive impact diminishes. This finding implies that companies should already focus on building PsyCap capabilities amongst their employees prior to the occurrence of information security incidents. According to our results, prevention rather than reaction strategies maximize the stress-reducing benefits of PsyCap in the workplace. Following the immediate occurrence of information security incidents, it is recommended to debrief the affected employees within the first 72 hours. During a critical incident stress debriefing, the victims are encouraged to express their feelings regarding the incident, receive confirmation for these feelings to be normal in such situations and that they are supported in assimilating the experience. Providing immediate assistance to the victims can disrupt or prevent the onset of more severe issues [37]. This could reduce the security-related stress employees build up after having become victims of cybercrime. We recommend organizations to supplement these acute debriefs with long-term PsyCap training to effectively mitigate SRS amongst their workforce.

While most previous studies found no significant effect of gender and age on PsyCap [41, 46, 59], we found older employees to demonstrate a slightly higher PsyCap. Since one's life experience increases with age, it is more likely that older employees had to overcome more challenges in their lives, allowing them to develop a more positive mental state.

5.2. Limitations and future work

As indicated in the analysis section, we had to eliminate two of the four sub-constructs of PsyCap during the factor analysis. To be able to study all aspects of PsyCap in the future, it is necessary to revise the respective items. Rephrasing them to distinguish their unique characteristics while maintaining their role within the overall PsyCap construct can increase the validity.

Future work can help identify other factors not considered in the current study that impinge the relationship between PsyCap and SRS. For instance, cultural factors [14], organizational commitment, and social influence [26] have been linked to improving employee's security behavior, so it remains to be tested to which extent these factors affect the security-related stress levels of employees as well.

To the best of our knowledge, no classification of security-related stressors with regard to their stress impact in the information security context exists. Future work can fill this research gap, which will benefit the investigation of SRS in the future tremendously.

According to D'Arcy and Teh [18], employees respond to security-related stress with adverse emotional reactions which, in turn, increase

neutralization of security policy violations and thereby decrease compliance behavior. Sommer et al. [61] link negative emotions to decreases in resilience, whereas positive emotions strengthen resilience. This can be explained by the supporting role positive emotions play in the recovery process from negative experiences. It has been shown that strong positive emotions can even replace negative ones [20]. It thus remains interesting to identify whether psychological capital creates positive emotions that are strong enough to suppress negative emotions associated with experiencing security incidents and dealing with strict security rules.

More importantly, changes over time represent an important factor not considered in our study. By applying a longitudinal approach, future work can investigate how PsyCap impacts individuals' stress-levels over time. We especially recommend focusing on causality when examining the relationship between these constructs. As reported by McCormac et al. [45], high stress levels do not necessarily translate to lower security awareness as resilience mediates this relationship. Future work can test whether PsyCap represents a similarly strong mediator.

As with any empirical study relying on self-reported data, our results are subject to response bias and social desirability bias. We attempted to counter these effects by carefully designing the questionnaire and ensuring anonymity and confidentiality. Moreover, we applied statistical techniques to identify dishonest reporting (e.g., we included control items to check if participants carefully read the instructions) and checked the validity and reliability of our results. Nevertheless, future work can further explore the concept of PsyCap following an experimental or a mixed-methods approach. For instance, Zhu et al. [70] created scenarios of encounters in a work environment to test the influence of humble leadership on employees' resilience.

Reichard et al. [57] placed PsyCap into the context of cross-cultural interactions, and Wernsing [68] applied a PsyCap measurement in twelve different national cultures while highlighting the importance of testing measurement invariances across cultures. Since all our participants are Americans, it remains unclarified how the construct of PsyCap performs in other cultures. The cultural context of our study thus represents a final limitation.

6. Conclusion

In contrast to existing psychological capital scales, the newly developed PsyCap items are explicitly targeted to psychological capabilities relevant to information security. This encompasses not only confidence in their abilities but also their ability to bounce back from challenges after information security incidents.

Building on previous research that associates PsyCap with multiple positive organizational outcomes, this study confirms desirable organizational security outcomes for the adapted PsyCap construct as well. Specifically, organizations can expect reductions in security-related stress when investing in building their employees' PsyCap. This provides a competitive advantage for organizations in a digitalized world, in which the frequency and severity of information security attacks continuously rise.

7. References

[1] Ament, C., and S. Haag, "How Information Security Requirements Stress Employees", *Proceedings of the 37th International Conference on Information Systems*, (2016), 3673–3689.

[2] American Psychological Association, "The Road to Resilience.", 2020. https://www.apa.org/helpcenter/road-resilience.

[3] Avey, J.B., R.J. Reichard, F. Luthans, and K.H. Mhatre, "Meta-Analysis of the Impact of Positive Psychological Capital on Employee Attitudes, Behaviors, and Performance", *Human Resource Development Quarterly 22*(2), 2011, pp. 127–152.

[4] Bandura, A., "Self-Efficacy Conception of Anxiety", *Anxiety Research 1*(2), 1988, pp. 77–98.

[5] Bandura, A., *Self-efficacy: The exercise of control*, Freeman, New York, 1997.

[6] Baron, R.A., R.J. Franklin, and K.M. Hmieleski, "Why Entrepreneurs Often Experience Low, Not High, Levels of Stress: The Joint Effects of Selection and Psychological Capital", *Journal of Management 42*(3), 2016, pp. 742–768.

[7] Berinsky, A.J., G.A. Huber, and G.S. Lenz, "Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk", *Political Analysis 20*(3), 2012, pp. 351–368.

[8] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly 34*(3), 2010, pp. 523–548.

[9] Burns, A.J., T.L. Roberts, C. Posey, and P.B. Lowry, "Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals", *Computers in Human Behavior 68*, 2017, pp. 190–209.

[10] Caniëls, M.C.J., and S.M.J. Baaten, "How a Learning-Oriented Organizational Climate is Linked to Different Proactive Behaviors: The Role of Employee Resilience",

Social Indicators Research 143(2), 2019, pp. 561–577.
[11] Çavuş, M.F., and A. Gokçen, "Psychological Capital: Definition, Components and Effects", *British Journal of Education, Society & Behavioural Science*, 2015, pp. 244–255.
[12] Chang, S.-H., H.-M. Hsu, Y. Li, and J.S.-C. Hsu, "The Influence of Information Security Stress on Security Policy Compliance: A Protection Motivation Theory Perspective", *Proceedings of the 22nd Pacific Asia Conference on Information Systems*, (2018).
[13] Chemers, M.M., L. -t. Hu, and B.F. Garcia, "Academic Self-Efficacy and First-Year College Student Performance and Adjustment", *Journal of Educational Psychology 93*(1), 2001, pp. 55–64.
[14] Connolly, L.Y., M. Lang, J. Gathegi, and D.J. Tygar, "Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study", *Information & Computer Security 25*(2), 2017, pp. 118–136.
[15] Cooper, C.L., and S. Cartwright, "Healthy Mind; Healthy Organization— A Proactive Approach to Occupational Stress", *Human Relations 47*(4), 1994, pp. 455–471.
[16] Cramer, R.J., T.M.S. Neal, and S.L. Brodsky, "Self-efficacy and confidence: Theoretical distinctions and implications for trial consultation", *Consulting Psychology Journal 61*(4), 2009, pp. 319–334.
[17] D'Arcy, J., T. Herath, and M.K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", *Journal of Management Information Systems 31*(2), 2014, pp. 285–318.
[18] D'Arcy, J., and P.-L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization", *Information & Management 56*(7), 2019, pp. 103–151.
[19] Frank, M., "Sharing Information Security Failure: The Role of Social Context and Social Environment", *Proceedings of the 24th Pacific Asia Conference on Information System*, (2020), 202.
[20] Fredrickson, B.L., and R.W. Levenson, "Positive Emotions Speed Recovery from the Cardiovascular Sequelae of Negative Emotions", *Cognition & Emotion 12*(2), 1998, pp. 191–220.
[21] Frese, M., and N. Keith, "Action Errors, Error Management, and Learning in Organizations", *Annual Review of Psychology 66*, 2015, pp. 661–687.
[22] Guo, K.H., and Y. Yuan, "The effects of multilevel sanctions on information security violations: A mediating model", *Information and Management 49*(6), 2012, pp. 320–326.
[23] Hair, J.F., B.J. Babin, R.E. Anderson, and W.C. Black, *Multivariate Data Analysis*, Pearson Education Limited, Harlow, Essex, 2014.
[24] Heartfield, R., and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework", *Computers and Security 76*, 2018, pp. 101–127.
[25] Herath, T., and H.R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems 47*(2), 2009, pp. 154–165.
[26] Herath, T., and H.R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems 18*(2), 2009, pp. 106–125.
[27] Huang, H.-W., N. Parolia, and K.-T. Cheng, "Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective", *Proceedings of the 20th Pacific Asia Conference on Information System*, 2016.
[28] Huang, L., and F. Luthans, "Toward Better Understanding of the Learning Goal Orientation- Creativity Relationship: The Role of Positive Psychological Capital", *Applied Psychology 64*(2), 2014, pp. 444–472.
[29] Hung, W.H., K. Chen, and C.P. Lin, "Does the proactive personality mitigate the adverse effect of technostress on productivity in the mobile environment?", *Telematics and Informatics 32*(1), 2015, pp. 143–157.
[30] Hwang, I., and O. Chao, "Examining technostress creators and role stress as potential threats to employees' information security compliance", *Computers in Human Behavior 81*, 2018, pp. 282–293.
[31] Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, (2012), 83–95.
[32] Johnston, A.C., and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly 34*(3), 2010, pp. 549–566.
[33] Klesel, M., N. Narjes, and B. Niehaves, "Conceptualizing IT Resilience: An Explorative Approach", *Multikonferenz Wirtschaftsinformatik*, (2018), 1008–1019.
[34] Kohn, V., "How Employees' Digital Resilience Makes Organizations More Secure", *Proceedings of the 24th Pacific Asia Conference on Information System*, (2020), 190.
[35] Kuntz, J., P. Connell, and K. Näswall, "Workplace resources and employee resilience: the role of regulatory profiles", *Career Development International 22*(4), 2017, pp. 419–435.
[36] Lee, C., C.C. Lee, and S. Kim, "Understanding information security stress: Focusing on the type of information security compliance activity", *Computers & Security 59*, 2016, pp. 60–70.
[37] Leonard, R., and L. Alison, "Critical incident stress debriefing and its effects on coping strategies and anger in a sample of Australian police officers involved in shooting incidents", *Work and Stress 13*(2), 1999, pp. 144–161.
[38] Lorenz, T., C. Beer, J. Pütz, and K. Heinitz, "Measuring Psychological Capital: Construction and Validation of the Compound PsyCap Scale (CPC-12)", *PloS ONE 11*(4), 2016, pp. 1–17.
[39] Luthans, F., B.J. Avolio, J.B. Avey, and S.M. Norman, "Positive psychological capital: Measurement and relationship with performance and satisfaction", *Personnel Psychology 60*(3), 2007, pp. 541–572.
[40] Luthans, F., and C.M. Youssef, "Human, Social, and Now Positive Psychological Capital Management",

Organizational Dynamics 33(2), 2004, pp. 143–160.
[41] Luthans, F., C.M. Youssef, D.S. Sweetman, and P.D. Harms, "Meeting the Leadership Challenge of Employee Well-Being Through Relationship PsyCap and Health PsyCap", *Journal of Leadership & Organizational Studies 20*(1), 2013, pp. 118–133.
[42] Luthar, S.S., D. Cicchetti, and B. Becker, "he Construct of Resilience: A Critical Evaluation and Guidelines for Future Work", *Child Development 71*(3), 2000, pp. 543–562.
[43] Malik, P., and P. Garg, "The relationship between learning culture, inquiry and dialogue, knowledge sharing structure and affective commitment to change", *Journal of Organizational Change Management 30*(4), 2017, pp. 610–631.
[44] Masten, A.S., "Ordinary magic: Resilience processes in development", *American Psychologist 56*(3), 2001, pp. 227–238.
[45] McCormac, A., D. Calic, K. Parsons, M. Butavicius, M. Pattinson, and M. Lillie, "The effect of resilience and job stress on information security awareness", *Information and Computer Security 26*(3), 2018, pp. 277–289.
[46] McMurray, A.J., A. Pirola-Merlo, J.C. Sarros, and M.M. Islam, "Leadership, climate, psychological capital, commitment, and wellbeing in a non-profit organization", *Leadership and Organization Development Journal 31*(5), 2010, pp. 436–457.
[47] Morgado, F.F.R., J.F.F. Meireles, C.M. Neves, A.C.S. Amaral, and M.E.C. Ferreira, "Scale development: Ten main limitations and recommendations to improve future research practices", *Psicologia: Reflexao e Critica 30*(1), 2017, pp. 1–20.
[48] Morony, S., S. Kleitman, Y.P. Lee, and L. Stankov, "Predicting achievement: Confidence vs self-efficacy, anxiety, and self-concept in Confucian and European countries", *International Journal of Educational Research 58*, 2013, pp. 79–96.
[49] Näswall, K., J. Kuntz, and S. Malinen, *Employee Resilience Scale (EmpRes): Technical Report*, 2015.
[50] Ole Johnsen, S., "Resilience at interfaces: Improvement of safety and security in distributed control systems by web of influence", *Information Management & Computer Security 20*(2), 2012, pp. 71–87.
[51] Owens, J., and E.M. Hawkins, "Using Online Labor Market Participants for Nonprofessional Investor Research: A Comparison of MTurk and Qualtrics Samples", *Journal of Information Systems 33*(1), 2019, pp. 113–128.
[52] Pastorino, E.E., and S.M. Doyle-Portillo, *What is psychology?: Foundations, Applications, and Integration*, Thompson Higher Education, Belmont, CA, 2009.
[53] Peterson, S.J., F. Luthans, B.J. Avolio, F.O. Walumba, and Z. Zhang, "Psychological Capital and Employee Performance: A Latent Growth Modeling Approach", *Personnel Psychology 46*(2), 2011, pp. 427–450.
[54] Ponemon Institute, "IBM: Cost of a Data Breach Report 2019", *Computer Fraud & Security 2019*(8), 2019, pp. 4.
[55] Posey, C., R.J. Bennett, T.L. Roberts, and P.B. Lowry, "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse", *Journal of Information System Security 7*(1), 2011, pp. 24–47.
[56] Puhakainen, P., and M. Siponen, "Improving employees' compliance through information systems security training: An action research study", *MIS Quarterly 34*(4), 2010, pp. 757–778.
[57] Reichard, R.J., M. Dollwet, and J. Louw-Potgieter, "Development of Cross-Cultural Psychological Capital and Its Relationship With Cultural Intelligence and Ethnocentrism", *Journal of Leadership & Organizational Studies 21*(2), 2014, pp. 150–164.
[58] Sheldon, K.M., and L. King, "Why Positive Psychology Is Necessary", *American Psychologist 56*(3), 2001, pp. 216–217.
[59] Singhal, H., and R. Rastogi, "Psychological capital and career commitment: the mediating effect of subjective well-being", *Management Decision 56*(2), 2018, pp. 458–473.
[60] Siponen, M., M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", *Information & Management 51*(2), 2014, pp. 217–224.
[61] Sommer, S.A., J.M. Howell, and C.N. Hadley, "Keeping Positive and Building Strength", *Group & Organization Management 41*(2), 2016, pp. 172–202.
[62] Stajkovic, A.D., and F. Luthans, "Self-Efficacy and Work-Related Performance: A Meta- Analysis", *Psychological Bulletin 124*(2), 1998, pp. 240–261.
[63] Tamjidyamcholo, A., M.S. Bin Baba, H. Tamjid, and R. Gholipour, "Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language", *Computers & Education 68*, 2013, pp. 223–232.
[64] Thomas, M., "Bullying among support staff in a higher education institution", *Health Education 105*(4), 2005, pp. 273–288.
[65] Tonkin, K., S. Malinen, K. Näswall, and J.C. Kuntz, "Building employee resilience through wellbeing in organizations", *Human Resource Development Quarterly 29*(2), 2018, pp. 107–124.
[66] Vance, A., M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory", *Information & Management 49*(3), 2012, pp. 190–198.
[67] Vogus, T.J., and K.M. Sutcliffe, "Organizational Resilience: Towards a Theory and Research Agenda", *International Conference on Systems, Man and Cybernetic*, (2007), 3418–3422.
[68] Wernsing, T., "Psychological Capital: A Test of Measurement Invariance Across 12 National Cultures", *Journal of Leadership & Organizational Studies 21*(2), 2014, pp. 179–190.
[69] Zajacova, A., S.M. Lynch, and T.J. Espenshade, "Self-Efficacy, Stress, and Academic Success in College", *Research in Higher Education 46*(6), 2005, pp. 677–706.
[70] Zhu, Y., S. Zhang, and Y. Shen, "Humble Leadership and Employee Resilience: Exploring the Mediating Mechanism of Work-Related Promotion Focus and Perceived Insider Identity", *Frontiers in Psychology 10*(673), 2019.