The Influence of Temporal Focus on Employee Preferences in Cybersecurity Training

Faheem Ahmed Shaikh
University of Jyväskylä, faheem.a.shaikh@jyu.fi

The Influence of Temporal Focus on Cybersecurity Training Preferences

Completed Research Paper

Faheem Ahmed Shaikh
University of Jyväskylä
Faculty of Information Technology
40014, Jyväskylä, Finland
shaikfas@jyu.fi

Abstract

This study investigates the impact of employees' temporal focus on the effectiveness of Security Education, Training, and Awareness (SETA) programs in organizations. Drawing on Construal Level Theory, the research examines the relationship between temporal focus, level of abstraction in information processing, and preferences for tactical or strategic cybersecurity training. Findings confirm that employees with a present temporal focus prefer tactical training, while those with a future temporal focus prefer strategic training. Concrete cybersecurity cognition mediates the relationship between present temporal focus and tactical training preference, while abstract cybersecurity cognition mediates the relationship between future temporal focus and strategic training preference. Results emphasize the importance of understanding individual preferences when designing and delivering cybersecurity training programs to maximize engagement. The study contributes to the SETA literature.

Keywords: SETA, training engagement, temporal focus, cybersecurity

Introduction

Security Education, Training, and Awareness (SETA) is a vital component of cybersecurity, as it aims to educate and train employees on best practices, policies, and behaviors required to protect an organization's information systems from cyber threats (Hu et al., 2022). It helps control information system misuse (Parker, 1998; Whitman, 2004) and is considered an important cybersecurity investment (Disparte & Furlow, 2017). The effectiveness of SETA programs relies on ongoing voluntary compliance from employees (Pham et al., 2019) and addresses the human aspect of cybersecurity, which is often considered the weakest link in securing information systems assets (Khando et al., 2021).

Research on training psychology indicates that in order to enhance the effectiveness of a training program, it is imperative to consider both individual learner characteristics and the design of the training material (Atkinson & Shiffrin, 1968; Kolb, 1984). Learning styles, prior knowledge, and personal interests influence how individuals engage with and process training content, leading to varying outcomes. For instance, some learners may excel in hands-on activities, while others may prefer to focus on abstract concepts (Kolb, 2014). Differences in cognitive processing affect how individuals interpret and retain information (Atkinson & Shiffrin, 1968), while selective attention directs their focus towards aspects they find most relevant. Personal experiences and mental frameworks also shape the construction of knowledge. As a result, to optimize the outcomes of training programs, it is crucial to consider individual learner attributes.

In the realm of cybersecurity, individuals may have different levels of expertise, cultural backgrounds, and learning preferences, all of which can influence their receptiveness to the SETA program's content (Khando et al., 2021; Puhakainen & Siponen, 2010). Not addressing individual differences could lead to a one-size-fits-all approach to SETA programs, which may not be suitable for diverse employee populations (Alyami et al., 2023). When SETA programs fail to adequately consider individual differences, they may not effectively engage employees in learning and adopting cybersecurity best practices (Alyami et al., 2023;

Reeves, Delfabbro, et al., 2021). As a result, employees may be less vigilant and more prone to human errors, which are recognized as the direct or indirect cause of the majority of security incidents (Khando et al., 2021). Such shortcomings in SETA programs could result, for instance, in individuals being underprepared to handle cybersecurity threats. It could also lead to overconfidence and complacency among employees, who may believe that they are adequately prepared to handle cybersecurity threats (Parsons et al., 2013; Reeves, Calic, et al., 2021). This sense of under preparedness, or false sense of security can exacerbate the organization's vulnerability to cyberattacks and make it difficult to establish a strong security posture. Puhakainen and Siponen (2010) argue that IS security policy compliance training should be theoretically driven and utilize learning tasks that are personally relevant to the learners, which can help in achieving the desired behavioral change.

Aligning SETA programs with unique learning needs therefore necessitates a more nuanced approach. One means of enhancing the match between learner requirements and SETA training content is to demarcate broad aspects of cybersecurity training and identify individual preferences for them. The paper proposes that differentiating tactical and strategic cybersecurity aspects in training and identifying individual learner preferences for either could contribute to enhancing the efficiency of SETA programs. Tactical training concentrates on imparting practical skills that employees can apply to prevent, identify, and respond to cybersecurity threats at a personal level. Examples include identifying phishing emails and adopting safe browsing habits. However, while tactical aspects are essential, they are not sufficient on their own. SETA programs serve not only as a valuable tool for instructing employees about the appropriate actions to take in relation to information security policies, but also as a means to enhance their understanding of the underlying principles and rationale for these policies (Lowry et al., 2015). Consequently, when employees lack a comprehensive understanding of the foundational concepts and justifications for information security policies, they may be more inclined to perceive modifications to these policies as arbitrary and unjust (Lowry et al., 2015). Given that cybersecurity threats are continuously changing and becoming more sophisticated, even as individuals stay susceptible despite training, it is not feasible to train individuals on every possible threat scenario. Filling this gap, training on strategic cybersecurity aspects provides employees with the broader context to be proactive against a broader and emerging range of possible threat scenarios. Training on strategic aspects encompasses the wider organizational security landscape, covering topics such as the rationale behind security policies, compliance, and secure data handling principles. While tactical aspects might require thinking in concrete terms, strategic aspects demand a more abstract understanding of cybersecurity concepts so that they can be operationalized in unforeseen scenarios.

Emphasizing only one of tactical or strategic cybersecurity aspects at the expense of the other has its own pros and cons. Focusing on tactical aspects ensures that employees are equipped to swiftly identify and address immediate threats. However, overemphasis on tactical aspects may result in employees neglecting the broader context of information security, limiting their ability to respond to new and emerging threats that they may not be familiar with. On the other hand, while an exclusive focus on strategic cybersecurity aspects might encourage employees to adopt a more comprehensive approach to risk management and gain a deeper understanding of various aspects of organizational security policies and compliance, it might cause them to overlook immediate cybersecurity threats.

Balancing training on tactical and strategic cybersecurity is vital for an organization's overall protection. Integrating both aspects into employee training ensures a comprehensive information security approach, allowing employees to maintain productivity while complying with security requirements (Padayachee, 2012 ; Warkentin et al., 2016). Addressing both task-specific and contextual knowledge fosters a security-aware culture that mitigates cybersecurity risks (Chen et al., 2015). Recognizing this distinction can enable organizations to develop tailored strategies and training programs.

Applying research on training psychology to this domain, it is entirely possible that individual learner characteristics, learning styles and personal interests will influence employee preferences to attend to either type of SETA training content. Therefore, when considering the tactical/strategic dichotomy of cybersecurity training in light of individual differences that impact training preferences, a key question arises: which individual differences influence employees' attention towards tactical versus strategic aspects of cybersecurity? Literature in cognitive psychology (Forster et al., 2004; Shipp et al., 2009) has found an association between individuals' predisposition to greater levels of present or future temporal focus and their predisposition to think in concrete or abstract terms. The research question therefore is: 'Do greater

levels of present or future temporal focus affect individuals' preference for either tactical or strategic aspects of cybersecurity training?'

Theoretical Background

SETA Programs

SETA programs focus on increasing awareness of security issues and enabling a deep understanding of why security protection is needed (Cram et al., 2019). Despite the importance of SETA, research has shown that most SETA programs are standardized and delivered with a one-size-fits-all approach (Dincelli & Chengalur-Smith, 2020). Traditional SETA programs tend to be narrowly focused on technical issues and lack context. This inadequacy in SETA programs contributes to security breaches and information security policy violations within organizations (Willison & Warkentin, 2013).

To improve SETA programs, it is vital to identify the target audience and tailor the content according to their needs (Tsohou et al., 2015), the organization's security policies, and the employees' knowledge level (Karjalainen & Siponen, 2011). Various studies stress the importance of measures such as personalization and user segmentation towards this objective (Fujs et al., 2021; Kam et al., 2021; Pattinson et al., 2019). In their most recent review of SETA literature, Hu et al. (2022) find that factors contributing to SETA success that have been investigated include senior manager support, media richness of delivery methods, use of persuasive messages, training duration, and game-based approaches among others. However, the critical role of individual differences in this specific area has received scarce attention.

Temporal Focus

Temporal focus refers to the relative importance of past, present, and future time frames in shaping an individual's thoughts and actions (Shipp et al., 2009). It is a crucial aspect of human cognition that influences how individuals perceive time and make decisions. It consists of three distinct dimensions—past, present, and future focus—that shape an individual's thoughts and actions in unique ways.

Individuals who have a present focus tend to emphasize immediate gratification, take increased risks, and formulate plans with shorter time horizons. They tend to concentrate on immediate situations, experiences, and emotions. They are more likely to prioritize short-term goals, immediate gratification, and tangible aspects of their lives. Present focus is associated with seizing opportunities and spontaneity (Shipp et al., 2009).

Those with a future focus are goal-oriented, make long-term plans, and consider future consequences (Ashkanasy et al., 2004; Nadkarni & Chen, 2014). They may be more strategic and plan-oriented and prioritize stability and security over immediate gratification.

Past focus involves reflecting on the past, using past memories in decision making, and learning from previous experiences (Holman & Silver, 1998; Shipp & Aeon, 2019). Individuals with greater past focus are more reflective and introspective.

Temporal focus is generally considered a stable individual cognitive characteristic, as individuals develop inclinations to focus on specific time periods to varying degrees over a period of time (Shipp et al., 2009; Zimbardo & Boyd, 2015). Factors that shape an individual's temporal focus include early childhood experiences and socioeconomic status (McGrath & Tschan, 2004). However, temporal focus can also change in reaction to critical life events (Shipp & Aeon, 2019). Despite its stability, individuals are often unaware of its subtle influence on their decisions and behaviors (Zimbardo & Boyd, 2015). Regardless of the default behavioral tendency, individuals can be made to alter their temporal focus momentarily in response to specific cues (Cojuharenco et al., 2011).

The study of temporal focus has evolved over time. In initial research, it was regarded as a continuum, with individuals principally focusing on either the past, the present, or the future (Nuttin, 2014). However, more recent research emphasizes that these three different foci are disparate dimensions instead of being at the opposite ends of a continuum, and classifying individuals into a single category may impose artificial boundaries (Shipp et al., 2009). Therefore, individuals may have greater or lesser levels of each temporal orientation within their overall temporal focus (Cojuharenco et al., 2011).

Temporal focus has demonstrated its predictive capacity in influencing a range of decisions that have implications for tasks, including how information is processed, plans are formulated, and decisions are made. (Kivetz & Tyler, 2007; Simons et al., 2004). Moreover, it affects attitudes, decisions, and behaviors, as demonstrated in research on goal-setting, motivation, performance, learning, affect, and strategic choice (Fried & Slowik, 2004; Wilson & Ross, 2003) Researchers can develop more accurate models of decision-making across various domains by understanding these differences. For instance, in the health domain, temporal focus has been linked to various health-related behaviors, such as diet, exercise, and substance use (Gellert et al., 2011; Keough et al., 1999; Laran, 2010). Individuals with a future focus may be more likely to adopt healthy behaviors and avoid risky ones, as they consider the long-term consequences of their actions.

Construal Level Theory

Temporal focus shapes an individual's prioritization of aspects of their experiences and environment, depending on whether they are past, present, or future-oriented. Construal Level Theory (CLT) offers a framework for explaining how people process and interpret information when they consider past, present or future scenarios. It sheds light on why individuals with varying temporal focus may selectively pay attention to different aspects of an issue.

CLT proposes that the psychological distance of an event influences how it is mentally represented, with distant events being construed more abstractly and near events being construed more concretely (Trope et al., 2007). Psychological distance encompasses various dimensions, such as temporal, spatial, hypothetical, and social distance. As events become more distant, they are represented by high-level construals, which focus on essential, abstract, and global features. In contrast, psychologically near events are represented by low-level construals, emphasizing peripheral, concrete, and local features (Trope et al., 2007). The relationship between psychological distance and abstraction arises from the association between direct experience and event information. When events occur in the "here and now," they are thought of in concrete terms using rich, contextualized detail. As events become more distant, the available information decreases, leading to more abstract and schematic representations (Liberman et al., 2007).

Higher levels of abstraction lead to greater focus on central features: When events and objects are perceived at higher levels of abstraction, individuals focus on the central, essential features of those events and objects. This reduces the influence of peripheral details and contextual information. Lower levels of abstraction lead to greater focus on contextual details: When events and objects are perceived at lower levels of abstraction, individuals focus on contextual details and peripheral features. This increases the influence of contextual information on perception and decision-making.

When events and objects are perceived at higher levels of abstraction, individuals tend to focus on the desirability of outcomes rather than their feasibility. On the other hand, lower levels of abstraction lead to greater preference for feasibility over desirability; this leads to a greater focus on practical considerations.

CLT has been used to explain individual decision-making in a variety of domains including health behavior, financial decision-making and financial decision-making. For instance, CLT has been used to explain how individuals construe environmental behaviors, such as recycling, energy conservation, and sustainable consumption (O'Connor & Keil, 2017; Reczek et al., 2018; Wang et al., 2019). For example, individuals with a high-level construal may focus on the long-term benefits of environmental behaviors, such as preserving the planet for future generations, whereas individuals with a low-level construal may focus on the immediate costs and benefits of engaging in these behaviors.

A few studies in IS have also used CLT. Lee et al. (2019) have applied it to the domain of IT project risk management; in this case, construal level refers to the extent to which IT project managers think about a project risk, or risk response in an abstract or concrete manner. This construal is then used to explain IT project managers' choices during risk management activities. Fard Bahreini et al. (2020) study how high- or low-level construal feedback messages can help to guide security performance of novice non-organizational users. In a qualitative study, (Jaeger et al., 2017) discuss how lowering psychological distance can help increase information security awareness.

Hypotheses

Construal level theory suggests that present-focused individuals engage in low-level construal, characterized by concrete thinking, focus on specific details, and feasibility thinking. This focus on tangible aspects and practicality leads them to seek solutions that are actionable and address perceived risks. Construal level can impact how individuals perceive cybersecurity threats. Specifically, low-level construal can be expected to engage individuals' focus on immediate threats and specific vulnerabilities, leading them to view cybersecurity as an urgent issue requiring swift action. As a result, it can be expected that such individuals will prioritize the high probability of cyberattacks in the short term, which will drive them to focus on actionable solutions that they can directly manage and execute.

Tactical training refers to the extent to which an individual understands a specific task or technology's capabilities (Munro et al., 1997; Nambisan et al., 1999; Sanchez & Heene, 1996). Tactical aspects of cybersecurity training, which focus on knowledge depth (Munro et al., 1997), provide employees with the skills to effectively address specific cybersecurity threats within immediate contexts. Employees with task-specific knowledge can effectively address threats within particular contexts (Safa & Von Solms, 2016), implement recommended security measures (Van Niekerk & Von Solms, 2010), and perform mitigating actions (Padayachee, 2012). Insufficient task-specific knowledge may lead to increased information security incidents involving employees. Employees with present temporal focus may be more receptive to training modules that emphasize practical guidance, such as recognizing and reporting phishing emails, safe web browsing and downloading, and strong password creation and management. Their preference for practical, immediate solutions aligns with the nature of tactical cybersecurity (Ifinedo, 2012; Van Niekerk & Von Solms, 2010) and may prioritize training that equips them to swiftly identify and address these threats.

In summary, employees with a present temporal focus are more likely to think in concrete terms and prioritize feasibility (Trope et al., 2007). This predisposes them to be interested in tactical cybersecurity training that emphasizes practical guidance and immediate solutions.

Hypothesis 1a: Present temporal focus is positively associated with greater preference for tactical cybersecurity training.

Hypothesis 1b: Concrete cybersecurity cognition is the mechanism through which individuals with present temporal focus will prefer tactical cybersecurity training.

Individuals with a future temporal focus engage in high-level construal, marked by abstract thinking (Liberman et al., 2007; Shani et al., 2009; Shipp et al., 2009). This abstract mindset allows them to perceive the broader picture and consider the context, fostering a more comprehensive approach to decision-making. This focus on abstract aspects of events and objects may lead individuals with a future temporal focus to pay greater attention to strategic cybersecurity aspects.

Strategic cybersecurity training, which is associated with contextual knowledge also known as know-what (Bierly & Chakrabarti, 1996; Sanchez & Heene, 1996), assists employees in comprehending a broad spectrum of varied information security threats, leading to comprehensive response strategies (Ashenden, 2008; Burns et al., 2017; Willison & Warkentin, 2013). Employees with future temporal focus may therefore be more receptive to training modules that emphasize a broader understanding of cybersecurity, such as the rationale behind organizational security policies, industry standards and compliance, and data classification and handling principles. Their preference for abstract thinking aligns with the nature of strategic cybersecurity (Posey et al., 2015). This broader perspective allows employees to assess the impacts of threats, identify risks beyond their immediate responsibilities, and adapt to evolving security landscapes (Posey et al., 2015).This ability to think in the long-term can be expected to allow individuals to appreciate the evolving nature of cybersecurity risks, understanding that new threats emerge over time and that the threat landscape is not limited to the present security posture. Insufficient context may limit threat recognition, leading employees to focus on strict policy adherence and habituation (Vance et al., 2012) rather than understanding the broader security consequences of their behavior.

Hypothesis 2a: Future temporal focus is positively associated with greater preference for strategic cybersecurity training.

Hypothesis 2b: Abstract cybersecurity cognition is the mechanism through which individuals with future temporal focus will prefer strategic cybersecurity training.

Method

Study 1

Sample:

For testing hypotheses H1a and H2a, a study was carried out at the South Asian branch office of a multinational financial services firm. 332 employees were invited via email to complete an online survey. They were informed that the company was planning to improve its security awareness and training efforts. Towards this end, their inputs were sought. In addition to the initial invite, they were also sent a reminder to complete the survey. 274 employees completed the online survey. 221 of these employees have taken part in the actual training. The participants in the final sample were 57.47% female. The average work experience was 11.65 years.

Measures:

Independent variable: Present and Future temporal focus: Temporal focus was measured using the 12-item scale developed by Shipp et al. (2009). The temporal focus scale is composed of three dimensions viz., past, present and future. Items for past temporal focus were used as a control variable. Example items are: "I think about what my future has in store" (Future), "My mind is on the here and now." (Present), "I reflect on what has happened in my life" (Past). Responses were obtained on a 7-point scale describing the frequency with which the respondent thought about the time frame indicated by the item (1 = never; 3 = sometimes; 5 = frequently; 7 = constantly).

Dependent variable: Cybersecurity training preference: Individuals were asked to choose three out of six training modules that they would be most interested in attending for the training. Of the options, three modules focus on strategic cybersecurity, while the other three emphasize practical know-how (tactical cybersecurity). Options for strategic cybersecurity included: Principles behind organizational Security Policies, Industry Standards and Compliance, and Data Classification and Handling Principles. Options for tactical cybersecurity included: Recognizing and Reporting Phishing Emails, Safe Web Browsing and Downloading, and Strong Password Creation and Management. Detailed information on the presentation of these options is shown in the Appendix. The dependent variable was coded 0 (tactical) or 1 (strategic) depending on the dominant number of modules chosen.

Control variables: Age (mean centered), gender (0 for Female, 1 for Male) and the following variables:

IT Education: An employee's educational background, particularly in areas such as computer science or information systems, may influence their preference for tactical or strategic cybersecurity training modules. Employees were therefore asked if they had any formal qualifications (degrees or certifications) in an information technology-related field. This was coded 0 for no, 1 for yes.

Prior training: Employees with recent cybersecurity training may have different training preferences than those without any prior exposure. Employees were therefore asked whether they underwent any cybersecurity training within the past three years. This was coded 0 for no, 1 for yes.

Past incident: Employees responded if they had been a victim of a cybersecurity attack during the past three years, resulting in tangible damage. This was coded 0 for no, 1 for yes.

The control variable questions were asked towards the end of the survey. Work experience was excluded from the analysis as it was highly correlated with Age and Gender.

Results:

Descriptive statistics for all variables are presented in Table 1. Logistic regression was used to test H1a and H2a. In Model 1 shown in Table 2, only the control variables were included. In Model2, control variables as well as the independent variables were included. H1a posits that Present temporal focus is positively associated with a preference for tactical cybersecurity training while H2a posits that future temporal focus is positively associated with a preference for strategic cybersecurity training. Regression results show that the coefficient for Future temporal focus is positive and significant. This lends support to H2a (β=0.572; S.E.=-0.176; $p<0.001$). Since the reference category for the dependent variable is preference for tactical

cybersecurity training, H1a is supported too, with the sign of the coefficient reversed (β=0.782; S.E.=0.155; p<0.001). The McFadden R^2 for the model is 20.6.

Variables	Mean	S.D.	1	2	3	4	5	6	7	8	9
1.Age	0.00	6.9	1								
2.Gender	0.43	0.5	-0.20**	1							
3.Work Ex.	11.65	6.5	0.98**	-0.21**	1						
4.IT Educ	0.39	0.5	-0.66**	0.02	-0.64**	1					
5.Prior training	0.13	0.3	0.10	-0.03	0.06	-0.19**	1				
6.Past incident	0.03	0.2	0.19**	0.03	0.21**	-0.13**	-0.06	1			
7.Past TF	3.70	1.1	0.23**	-0.10	0.19**	-0.19**	0.03	-0.18**	1		
8.Present TF	4.63	1.1	-0.10	0.10	-0.11*	0.05	0.10	-0.14*	0.14*	1	
9.Future TF	4.43	1.1	0.03	0.12*	0.05	-0.05	0.16*	0.16**	-0.28**	0.01	1
10.CSTP	0.34	0.5	0.14*	-0.09	0.16*	-0.03	-0.07	0.18**	-0.17*	-0.4**	0.22**

n=221, ** p < 0.01, * p<0.05, TF: Temporal Focus, IT Educ: IT Education

CSTP: Cybersecurity Training preference

Table 1. Descriptive Statistics

Study 2

Sample:

The relationship between temporal focus and level of construal has been well-established in literature in various domains (Labroo & Patrick, 2009; Spassova & Lee, 2013; Trope et al., 2007). Study 2 was therefore carried out to establish the association between construal level and preference for cybersecurity training. The objective here was to manipulate the level of mental construal, either abstract or concrete, through a manipulation task. This is to establish that concrete or abstract construal is indeed the mechanism at play. The study was carried out using Mechanical Turk. 265 individuals completed an online survey. After eliminating non-usable responses for reasons described in the following paragraphs, the final sample had 190 responses. The average age of respondents was 29 years, average work experience was 7.6 years and 36.84% of the sample was female.

Individuals were randomly assigned to one of two conditions: Concrete or Abstract cybersecurity cognition. For this, they were first asked to answer a priming question. In the concrete cybersecurity cognition condition, they were asked: ”For answering the following two questions, imagine that you are working for an organization. In your **day-to-day activities**, what security measures or tools do you use to protect your devices and information from cyber threats?”

Variables **DV: Cybersecurity training preference**	**Model 1**	**Model 2**
Age	0.064** (-0.031)	0.061* (-0.033)
Gender	-0.368 (0.317)	-0.41 (0.355)
IT Education	0.308 (0.423)	0.455 (0.448)
Prior training	-0.485 (0.488)	-0.574 (-0.516)
Past incident	1.613 (1.163)	0.922 (-1.227)
Past temporal focus	-0.413*** (0.154)	-0.151 (-0.174)
Present temporal focus		-0.782*** (-0.155)
Future temporal focus		0.572*** (-0.176)
Constant	0.856 (0.65)	0.857 (1.197)
*** p<0.01, ** p<0.05, * p<0.1 Standard errors in parentheses		

Table 2. Hypothesis testing results

Individuals were randomly assigned to one of two conditions: Concrete or Abstract cybersecurity cognition. For this, they were first asked to answer a priming question. In the concrete cybersecurity cognition condition, they were asked: "For answering the following two questions, imagine that you are working for an organization. In your **day-to-day activities**, what security measures or tools do you use to protect your devices and information from cyber threats?"

In the abstract cybersecurity cognition condition, they were asked: "For answering the following two questions, imagine that you are working for an organization. At a **broader** level, how does awareness of the overall cybersecurity environment and potential risks influence how you protect yourself or your organization from cyber threats?"

In other areas of research too, manipulation of abstract or concrete cognition has been done by asking respondents to engage in qualitative activities. For example, Park and Hedgcock (2016) ask respondents to group objects and decipher abstract construal as a lesser number of groups. Huang et al. (2016) code individual sentences in online reviews based on whether they mention something concrete or abstract.

Following this, individuals were described a hypothetical scenario similar to the actual one in Study 1 and asked to choose three out of six training modules they would be most interested in attending for the training.

Finally, they were asked questions related to control variables: age, gender, work experience, IT Education, prior training, and whether they had been a victim of a cyberattack during the past three years.

The first author and a research assistant then independently coded responses to the priming condition question to ensure that respondents were indeed primed to the concrete or abstract cybersecurity cognition condition. The inter-rater agreement was 88.42%. Disagreements were resolved through discussion. Similar approach using manual coding of qualitative responses has been used extensively in past literature. Sample responses to the concrete cybersecurity cognition condition are: "I have enabled two-factor

authentication for my email account" and "I am using a password manager to keep my login information safe". Sample responses to the abstract cybersecurity cognition condition are: "I will speak up more and advocate about cybersecurity to my colleagues" and "I will probably understand when security is insufficient and discuss with a colleague or system administrator group about this". Respondents whose responses were not aligned with the priming condition were removed from the analysis. This left 190 valid responses.

Results:

Descriptive statistics for all variables are shown in Table 3. A chi square test was performed to check for the difference in means of the two categorical variables. Table 4 show a cross-tabulation for the two variables: Cybersecurity cognition and Cybersecurity training preference along with actual and expected frequencies. In the concrete cybersecurity cognition condition, individuals were significantly more likely to report a preference for tactical cybersecurity training, 80.17% vs. 19.82%, chi2=29.20, p<0.001. In the abstract cybersecurity cognition condition, individuals were significantly more likely to report a preference for strategic cybersecurity training, 58.10% vs. 41.89%.

Variables	**Mean**	**S.D.**	**1**	**2**	**3**	**4**	**5**
1. Age	29.079	4.259	1				
2. Gender	0.632	0.484	-0.117*	1			
3. Work experience	7.600	4.207	0.972***	-0.109	1		
4. IT Education	0.174	0.380	-0.139*	0.033	-0.099	1	
5. Cybersecurity cognition	0.389	0.489	-0.114	0.163**	0.022	0.061	1
6. Cybersecurity training preference	0.347	0.477	0.348***	0.007	0.457***	0.074	0.392***
n=190, *** p < 0.01, ** p<0.05, * p<0.1							

Table 3. Descriptive Statistics

Cybersecurity cognition	**Cybersecurity training preference**		
	Tactical	**Strategic**	**Total**
Concrete	93	23	116
(Expected)	75.7	40.3	
Abstract	31	43	74
(Expected)	48.3	25.7	
Total	124	66	190

Table 4. Hypothesis testing Cross-tabulation

Post-hoc analysis

In the following months, employees underwent cybersecurity training in batches. For assessing actual employee behavior, employee engagement with training was measured. For this, employees were provided with a link to a short online quiz that they could complete any time over the two weeks following training. This consisted of ten multiple choice questions related to the training. They were informed that taking the quiz was voluntary and was meant to reinforce the learning through self-assessment and feedback. Actual engagement was measured as 1 if the quiz was submitted, and 0 otherwise. To control for the effect of individual propensity to take a quiz, employees were informed that they could voluntarily take a general cybersecurity quiz before the training. This was measured as 1 if it was submitted, 0 otherwise.

Additional employees attended both tactical and strategic cybersecurity sessions, in addition to the ones that were initially asked for their training preference. Such additional trainees served as controls in the

analysis. This ensured that those that had shown a preference for either training would not resent being not offered a session of their choice. They were not asked at any point for their training preference. Same variables as those used in Study 1 were obtained from them following the training sessions. In addition to pre-training assessment, the analysis also controls for whether the employee was in the "treatment" group or the control group.

As indicated in Table 5, present (β=0.675; S.E.=0.223; p<0.001) and future temporal focus (β=0.596; S.E.=0.203; p<0.001) were both found to be positively associated with engagement with tactical cybersecurity training. On the other hand, while future temporal focus was found to be positively associated (β=0.815; S.E.=0.230; p<0.001) with strategic cybersecurity training, present temporal focus was found to be negatively associated (β=-0.539; S.E.=0.198; p<0.001).

Variable	**Training engagement: Tactical**	**Training engagement: Strategic**
Age	0.042 (0.037)	-0.046 (0.043)
Gender	0.236 (0.383)	0.036 (0.430)
IT Education	0.521 (0.433)	-0.882 (0.490)
Prior training	-0.033 (0.647)	-1.119 (0.803)
Past incident	0.46 (0.901)	-0.212 (1.090)
Past temporal focus	-0.249 (0.217)	-0.146 (0.222)
Present temporal focus	0.675*** (0.223)	-0.539*** (0.198)
Future temporal focus	0.596*** (0.203)	0.815*** (0.230)
Pre-training assessment	2.356*** (0.419)	2.184*** (0.481)
Treatment	-0.354 (0.438)	-0.595 (0.495)
Constant	-4.936*** (1.778)	-1.038 (1.563)
*** p<0.01, ** p<0.05, * p<0.1 Standard errors in parentheses		

Table 5: Post-hoc analysis

Discussion

The motivation for this study stems from the objective of understanding the impact of employees' temporal focus on their engagement with Security Education, Training, and Awareness (SETA) programs in organizations. Given the critical importance of cybersecurity and the need for organizations to foster a security-aware culture, it is crucial to examine factors that could influence the success of SETA programs.

Construal Level Theory (CLT) is an appropriate theoretical lens to develop arguments for the hypotheses because it directly addresses the relationship between temporal focus and the level of abstraction at which individuals process information. This level of information processing has potential implications for individual preferences (Trope et al., 2007). Our findings support Hypotheses 1a and 2a, which posited that present temporal focus would be positively associated with a preference for tactical cybersecurity training, while future temporal focus would be positively associated with a preference for strategic cybersecurity training.

The findings also support Hypotheses 1b and 2b, which proposed that concrete cybersecurity cognition would mediate the relationship between present temporal focus and preference for tactical training, while abstract cybersecurity cognition would mediate the relationship between future temporal focus and preference for strategic training. This suggests that individuals with a present temporal focus prioritize concrete, immediate solutions, whereas those with a future temporal focus emphasize a broader, more abstract understanding of cybersecurity concepts. This model is grounded in previous research that highlights the importance of tailoring training programs to individual preferences to maximize their effectiveness (Atkinson & Shiffrin, 1968; Kolb, 2014).

The post-hoc analyses show that such temporal foci also translate into actual behavioral engagement. While only present temporal focus could be expected to result in higher engagement with tactical training, the analysis shows that greater levels of future temporal focus too are associated with greater engagement with tactical cybersecurity training. A possible explanation is that tactical training usually entails hands-on skills, immediate problem-solving and direct skill application. Such skills will have universal appeal, especially in cybersecurity, where the ultimate outcome of abstract knowledge and concepts is also expected to be a tangible reduction in cybersecurity incidents. Interestingly, while a future temporal focus naturally aligns with greater engagement in strategic cybersecurity training, the present temporal focus appears to be inversely related to it. This negative correlation might stem from a resistance to abstract cybersecurity concepts amongst those with a pronounced present temporal focus, favoring tangible skills instead. Given this, organizations could benefit from initially exempting these individuals from conceptual cybersecurity training. Prioritizing training that imparts tangible skills may enhance initial engagement with SETA programs.

The findings of this study have several practical implications for organizations seeking to enhance their SETA programs. First, by conducting initial assessments to determine the dominant temporal focus of employees, organizations can tailor their training programs to better align with individual preferences, which may lead to increased engagement and more effective learning outcomes. This is especially relevant as factors such as cyber fatigue have been shown to hamper employee engagement with SETA programs (Reeves, Delfabbro, et al., 2021). While both aspects of cybersecurity training are important, prioritizing the preferred ones to enhance engagement and following it up with the secondary modules could be a good strategy.

Second, while a lot of focus in SETA programs is on imparting practical skills, organizations might benefit from understanding the tactical and strategic cybersecurity training. This can help to ensure that employees develop a comprehensive understanding of cybersecurity principles and practices, enabling them to respond effectively to a wide range of threat scenarios. Integrating both tactical and strategic training may also promote a more security-aware culture within the organization, mitigating overall cybersecurity risk (Chen et al., 2015). Moreover, as the cybersecurity landscape in an organization evolves as a result of changes such as mergers or adherence to new compliance standards, organizations can be mindful that SETA programs incorporate these changes in training modules instead of exclusively focusing on imparting the same practical skills.

The study's findings also suggest that organizations should be mindful of potential cognitive biases that may emerge as a result of employees' temporal focus. For example, employees with a present temporal focus may be more prone to overlooking the broader context of information security, while those with a future temporal focus may neglect immediate threats. This presents an interesting avenue for future empirical research. By addressing these biases in training, organizations can help to ensure that their employees maintain a balanced and effective approach to cybersecurity.

Contribution

This study contributes to the understanding of the role of individual differences in SETA programs, an essential component of effective cybersecurity management. While past research has studied multiple individual differences as antecedents to cybersecurity behaviors and attitudes, research on individual differences influencing SETA programs delivery is scarce (Alotaibi et al., 2016). For instance, cybersecurity literature highlights the critical role of individual differences in shaping attitudes and behaviors related to security policy compliance and situational information security awareness (Salmon et al., 2008; Shropshire et al., 2015). As Hu et al. (2022) highlight in their most recent review of SETA literature, factors contributing to SETA success that have been investigated include senior manager support, media richness of delivery methods, use of persuasive messages, duration, and game-based approaches among others. However, the critical role of individual differences in this specific area has received scarce attention. The study extends this literature by theorizing how temporal focus, an important individual difference, can affect cybersecurity training preferences through either concrete or abstract levels of construals about cybersecurity training.

The study also contribute by contextualizing (Makadok et al., 2018) construal level theory to the specific area of SETA programs. This contextualization has allowed uncovering new insights into how SETA programs can be segmented based on individual preferences. The finding that the universal appeal of tactical cybersecurity training leads to better individual engagement regardless of individual temporal focus, delineates boundary conditions specific to research on SETA programs.

Conclusion

In conclusion, our study highlights the crucial role of employees' temporal focus in determining the their preferences for Security Education, Training, and Awareness (SETA) programs in organizations. Our research confirms the hypotheses that employees with a present temporal focus tend to show higher preference for tactical training, while those with a future temporal focus exhibit greater preference for strategic cybersecurity training. These findings emphasize the importance of understanding individual preferences when designing and delivering cybersecurity training programs, as doing so can maximize engagement.

Future research could study several variables that could influence the dynamics of the hypothesized relationships. For instance, the incidence of recent major cybersecurity events within a company or its industry peers could transiently recalibrate employees' temporal focus towards the present, necessitating immediate remedial actions. The industry might have an effect too. Sectors with strict regulations, like healthcare, might focus more on preparing for the future, and employees might be relatively more focused on abstract concepts that need to be contextualized to local requirements, especially when dealing with sensitive data and compliance requirements. Similarly, the expectations of stakeholders and the pace of technological advancements in an industry can guide whether the focus is on the present or the future. In industries quick to adapt to new technologies, employees might lean towards a future focus, aiming to prepare for unknown cyber threats and seeking a deeper understanding of potential issues.

References

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal of Information Security Research, 6*(2), 660-666.

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for security education, training and awareness (SETA) program effectiveness: A lifecycle model. *Information Technology & People, 36*(8), 94-125. https://doi.org/10.1108/ITP-07-2022-0515

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201. https://doi.org/https://doi.org/10.1016/j.istr.2008.10.006

Ashkanasy, N. M., Gupta, V., Mayfield, M. S., & Trevor-Roberts, E. (2004). Future orientation.

Atkinson, R. C., & Shiffrin, R. M. (1968). Human memory: A proposed system and its control processes. In K. W. Spence & J. T. Spence (Eds.), *Psychology of learning and motivation* (Vol. 2, pp. 89-195). Academic Press. https://doi.org/10.1016/S0079-7421(08)60422-3

Bierly, P., & Chakrabarti, A. (1996). Generic knowledge strategies in the us pharmaceutical industry. *Strategic Management Journal, 17*, 123-135. https://doi.org/10.1002/smj.4250171111

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209. https://doi.org/10.1016/j.chb.2016.11.018

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19. https://doi.org/10.1080/08874417.2015.11645767

Cojuharenco, I., Patient, D., & Bashshur, M. R. (2011). Seeing the "forest" or the "trees" of organizational justice: Effects of temporal perspective on employee concerns about unfair treatment at work. *Organizational Behavior and Human Decision Processes, 116*(1), 17-31. https://doi.org/10.1016/j.obhdp.2011.05.008

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525-+. https://doi.org/10.25300/misq/2019/15117

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems, 29*(6), 669-687. https://doi.org/10.1080/0960085x.2020.1797546

Disparte, D., & Furlow, C. (2017). The best cybersecurity investment you can make is better training. *Harvard Business Review, 5*.

Fard Bahreini, A., Cavusoglu, H., & Cenfetelli, R. (2020). *Role of feedback in improving novice users' security performance using construal level and valance framing* ICIS 2020,

Forster, J., Friedman, R. S., & Liberman, N. (2004). Temporal construal effects on abstract and concrete thinking: Consequences for insight and creative cognition. *Journal of Personality and Social Psychology, 87*(2), 177-189. https://doi.org/10.1037/0022-3514.87.2.177

Fried, Y., & Slowik, L. H. (2004). Enriching goal-setting theory with time: An integrated approach. *Academy of Management Review, 29*(3), 404-422.

Fujs, D., Vrhovec, S., & Vavpotic, D. (2021). Know your enemy: User segmentation based on human aspects of information security. *IEEE Access, 9*, 157306-157315. https://doi.org/10.1109/access.2021.3130013

Gellert, P., Ziegelmann, J. P., Lippke, S., & Schwarzer, R. (2011). Future time perspective and health behaviors: Temporal framing of self-regulatory processes in physical exercise and dietary behaviors. *Annals of Behavioral Medicine, 43*(2), 208-218. https://doi.org/10.1007/s12160-011-9312-y

Holman, E. A., & Silver, R. C. (1998). Getting "stuck" in the past: Temporal orientation and coping with trauma. *Journal of Personality and Social Psychology, 74*(5), 1146-1163. https://doi.org/10.1037/0022-3514.74.5.1146

Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems, 62*(4), 752-764. https://doi.org/10.1080/08874417.2021.1913671

Huang, N., Burtch, G., Hong, Y. L., & Polman, E. (2016). Effects of multiple psychological distances on construal and consumer evaluation: A field study of online reviews. *Journal of Consumer Psychology, 26*(4), 474-482. https://doi.org/10.1016/j.jcps.2016.03.001

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Jaeger, L., Ament, C., & Eckhardt, A. (2017). *The closer you get the more aware you become–a case study about psychological distance to information security incidents* ICIS 2017,

Kam, H., Ormond, D. K., Menard, P., & Crossler, R. E. (2021). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal, 32*(4), 888-926. https://doi.org/10.1111/isj.12374

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.

Keough, K. A., Zimbardo, P. G., & Boyd, J. N. (1999). Who's smoking, drinking, and using drugs? Time perspective as a predictor of substance use. *Basic and Applied Social Psychology, 21*(2), 149-164. https://doi.org/10.1207/S15324834BA210207

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/https://doi.org/10.1016/j.cose.2021.102267

Kivetz, Y., & Tyler, T. R. (2007). Tomorrow I'll be me: The effect of time perspective on the activation of idealistic versus pragmatic selves. *Organizational Behavior and Human Decision Processes, 102*(2), 193-211. https://doi.org/10.1016/j.obhdp.2006.07.002

Kolb, D. A. (1984). Experience as the source of learning and development. *Upper Sadle River: Prentice Hall*.

Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development*. FT press.

Labroo, A. A., & Patrick, V. M. (2009). Psychological distancing: Why happiness helps you see the big picture. *Journal of Consumer Research, 35*(5), 800-809. https://doi.org/10.1086/593683

Laran, J. (2010). Choosing your future: Temporal distance and the balance between self-control and indulgence. *Journal of Consumer Research, 36*(6), 1002-1015. https://doi.org/10.1086/648380

Lee, J. S., Keil, M., & Shalev, E. (2019). Seeing the trees or the forest? The effect of IT project managers' mental construal on IT project risk management activities. *Information Systems Research, 30*(3), 1051-1072. https://doi.org/10.1287/isre.2019.0853

Liberman, N., Trope, Y., & Wakslak, C. (2007). Construal level theory and consumer behavior. *Journal of Consumer Psychology, 17*(2), 113-117. https://doi.org/10.1016/s1057-7408(07)70017-7

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-230. https://doi.org/10.1111/isj.12063

Makadok, R., Burton, R., & Barney, J. (2018). A practical guide for making theory contributions in strategic management. *Strategic Management Journal, 39*(6), 1530-1545. https://doi.org/10.1002/smj.2789

McGrath, J. E., & Tschan, F. (2004). *Temporal matters in social psychology: Examining the role of time in the lives of groups and individuals*. American Psychological Association. https://doi.org/10.1037/10659-000

Munro, M. C., Huff, S. L., Marcolin, B. L., & Compeau, D. R. (1997). Understanding and measuring user competence. *Information & Management, 33*(1), 45-57. https://doi.org/10.1016/S0378-7206(97)00035-9

Nadkarni, S., & Chen, J. H. (2014). Bridging yesterday, today, and tomorrow: CEO temporal focus, environmental dynamism, and rate of new product introduction. *Academy of Management Journal, 57*(6), 1810-1833. https://doi.org/10.5465/amj.2011.0401

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. *MIS Quarterly, 23*(3), 365-395. https://doi.org/10.2307/249468

Nuttin, J. (2014). *Future time perspective and motivation: Theory and research method*. Psychology Press.

O'Connor, J., & Keil, M. (2017). The effects of construal level and small wins framing on an individual's commitment to an environmental initiative. *Journal of Environmental Psychology, 52*, 1-10. https://doi.org/10.1016/j.jenvp.2017.04.010

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680. https://doi.org/10.1016/j.cose.2012.04.004

Park, J., & Hedgcock, W. M. (2016). Thinking concretely or abstractly: The influence of fit between goal progress and goal construal on subsequent self-regulation. *Journal of Consumer Psychology, 26*(3), 395-409. https://doi.org/10.1016/j.jcps.2015.12.003

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. Security and Privacy Protection in Information Processing Systems, Berlin, Heidelberg.

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information Computer Security, 28*(1), 1-14. https://doi.org/10.1108/ics-01-2019-0022

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2019). Enhancing cyber security behavior: An internal social marketing approach. *Information & Computer Security, 28*(2), 133-159. https://doi.org/10.1108/ICS-01-2019-0023

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214. https://doi.org/10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757-778.

Reczek, R. W., Trudel, R., & White, K. (2018). Focusing on the forest or the trees: How abstract versus concrete construal level predicts responses to eco-friendly products. *Journal of Environmental Psychology, 57*, 87-98. https://doi.org/https://doi.org/10.1016/j.jenvp.2018.06.003

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity training. *Computers & Security, 106*, 102281. https://doi.org/10.1016/j.cose.2021.102281

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *Sage Open, 11*(1), 21582440211000049. https://doi.org/10.1177/21582440211000049

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. https://doi.org/10.1016/j.chb.2015.12.037

Salmon, P. M., Stanton, N. A., Walker, G. H., Baber, C., Jenkins, D. P., McMaster, R., & Young, M. S. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science, 9*(4), 297-323. https://doi.org/10.1080/14639220701561775

Sanchez, R., & Heene, A. (1996). Managing articulated knowledge in competence-based competition. In *Strategic learning and knowledge management* (pp. 163-187). John Wiley & Sons.

Shani, Y., Igou, E. R., & Zeelenberg, M. (2009). Different ways of looking at unpleasant truths: How construal levels influence information search. *Organizational Behavior and Human Decision Processes, 110*(1), 36-44. https://doi.org/10.1016/j.obhdp.2009.05.005

Shipp, A. J., & Aeon, B. (2019). Temporal focus: Thinking about the past, present, and future. *Current Opinion in Psychology, 26*, 37-43. https://doi.org/10.1016/j.copsyc.2018.04.005

Shipp, A. J., Edwards, J. R., & Lambert, L. S. (2009). Conceptualization and measurement of temporal focus: The subjective experience of the past, present, and future. *Organizational Behavior and Human Decision Processes, 110*(1), 1-22. https://doi.org/10.1016/j.obhdp.2009.05.001

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191. https://doi.org/https://doi.org/10.1016/j.cose.2015.01.002

Simons, J., Vansteenkiste, M., Lens, W., & Lacante, M. (2004). Placing motivation and future time perspective theory in a temporal perspective. *Educational Psychology Review, 16*(2), 121-139. https://doi.org/10.1023/B:EDPR.0000026609.94841.2f

Spassova, G., & Lee, A. Y. (2013). Looking into the future: A match between self-view and temporal distance. *Journal of Consumer Research, 40*(1), 159-171. https://doi.org/10.1086/669145

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology, 17*(2), 83-95. https://doi.org/10.1016/s1057-7408(07)70013-x

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58. https://doi.org/10.1057/ejis.201327

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

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

Wang, S., Hurlstone, M. J., Leviston, Z., Walker, I., & Lawrence, C. (2019). Climate change from a distance: An analysis of construal level and psychological distance from climate change. *Frontiers in Psychology, 10*, 22, Article 230. https://doi.org/10.3389/fpsyg.2019.00230

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25-35. https://doi.org/10.1016/j.dss.2016.09.013

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Wilson, A., & Ross, M. (2003). The identity function of autobiographical memory: Time is on our side. *Memory, 11*(2), 137-149. https://doi.org/10.1080/741938210

Zimbardo, P. G., & Boyd, J. N. (2015). Putting time in perspective: A valid, reliable individual-differences metric. In M. Stolarski, N. Fieulaine, & W. van Beek (Eds.), *Time perspective theory; review, research and application: Essays in honor of philip g. Zimbardo* (pp. 17-55). Springer International Publishing. https://doi.org/10.1007/978-3-319-07368-2_2

Appendix

Cybersecurity training preferences (Study 1)

Instructions: Please read the following security training module descriptions and choose three that you would be most interested in attending. As described, some modules focus on general cybersecurity principles, while others emphasize practical know-how and technical actions. Your input will help us design a training program that meets your needs and interests.

Key Principles of Organizational Security Policies: This module will provide an overview of the principles behind our organization's security policies and guidelines, and how they contribute to a secure working environment.

Compliance for Cybersecurity: This module will cover the key cybersecurity regulations and standards our organization must comply with, and the principles that underlie these requirements.

Key Principles of Secure Data Classification and Handling: This module will introduce you to the principles of data classification within our organization and the rationale for handling, storing, and sharing different types of data securely.

Recognizing and Reporting Phishing Emails: This module will teach you the practical steps to identify phishing emails, understand the risks they pose, and follow the appropriate procedures for reporting suspicious emails to the security team.

Safe Web Browsing and Downloading: This module will provide hands-on training on securely browsing the internet and downloading files, while reducing the risk of malware infections or data breaches.

Strong Password Creation and Management: This module will offer practical guidance on creating complex and unique passwords for all your accounts, as well as the importance of regularly updating your passwords and using secure password management tools.

Please select three modules you are most interested in attending:

[ ] Key Principles of Organizational Security Policies

[ ] Compliance for Cybersecurity

[ ] Key Principles of Secure Data Classification and Handling

[ ] Recognizing and Reporting Phishing Emails

[ ] Safe Web Browsing and Downloading

[ ] Strong Password Creation and Management

Click "Submit" to complete the questionnaire. Thank you for your input! Your responses will help us design a more effective and relevant security training program.