Received 8 August 2024
Revised 20 December 2024
23 January 2025
7 February 2025
Accepted 6 March 2025

Training for improved information security culture: a longitudinal randomized controlled trial

Martin Grill
Department of Psychology, University of Gothenburg, Gothenburg, Sweden

Teodor Sommestad and Henrik Karlzén
Department of Information Security and IT Architecture, Swedish Defence Research Agency (FOI), Linköping, Sweden, and

Anders Pousette
Department of Psychology, University of Gothenburg, Gothenburg, Sweden

Abstract

Purpose – The information security behaviors of individuals can pose a risk to their organization's information security. To address employees' information security behaviors and managers' information security leadership behaviors, this paper aims to develop a behavioral training program called Training for Improved Information Security Culture (TIISC). TIISC consisted of information-security training for the employees and managerial behavioral training for the managers. The training program aimed at direct change of behavior as well as indirect change through improved information security culture, as manifested through information security climate.

Design/methodology/approach – The effects of TIISC on information security culture was assessed in a longitudinal randomized controlled trial. Data were collected over a 16-month period, using both behavioral measurements and questionnaires on behavior and climate. Latent growth modeling was used for the statistical analysis of change, in terms of how change differed between the control and experimental groups.

This research was funded by the Swedish Civil Contingencies Agency, MSB. The funding sponsor's grant agreement required that the participants should be employees of Swedish organizations in societally important sectors. The funding sponsor did not have any other role in the study design, in the data collection, analysis or interpretation, in writing the report, or in the decision to submit the article for publication.

Credit author statement: Martin Grill: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Writing – review and editing, Funding acquisition.

Teodor Sommestad: Conceptualization, Methodology, Data Curation, Investigation, Writing – original draft, Writing – review and editing, Project administration, Funding acquisition.

Henrik Karlzen: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review and editing, Project administration, Funding acquisition.

Anders Pousette: Conceptualization, Methodology, Data Curation, Investigation, Funding acquisition.

Information & Computer Security
Vol. 33 No. 5, 2025
pp. 690-718
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-08-2024-0189

Findings – The results show that the training program had significant positive effects on the information security leadership of managers; but for employees, significant positive effects were only found for information security learning. Training programs that incorporate managerial behavioral training can realize important improvements in organizations' information security culture, primarily by addressing managers' information security leadership behaviors through behavior analysis and practice with performance feedback.

Originality/value – The authors report the results of a longitudinal randomized controlled trial testing the effects of information security training on multiple types of information security behaviors and approaches as indicators of information security culture. Longitudinal randomized controlled trials in security education training and awareness research are important because they advance the understanding of how information security culture can be effectively improved.

Keywords Information security culture, Training, Information security leadership, Information security behavior, Longitudinal study, Randomized controlled trial

Paper type Research paper

1. Introduction

The behaviors of individuals pose a risk to their organization's information security in many ways. For example, employees may threaten information security when they open phishing emails, surf malicious websites, connect infected USB sticks or move information to their private computers. However, there has historically been a lack of behavioral information security research. Crossler *et al.* (2013, p. 90) stated that "although a predominant weakness in properly securing information assets is the individual user within an organization, much of the focus of extant security research is on technical issues," and outlined directions for research on behavioral information security. Since then, several studies have addressed human behavior in relation to information security: Guo (2013) reviewed 17 papers on information security behaviors and categorized them into security assurance behavior, security compliant behavior, security risk-taking behavior and security damaging behavior; Cram *et al.* (2019) reviewed 95 papers on security compliance behavior; and Sommestad and Karlzén (2019) reviewed 48 field studies of phishing susceptibility. The research directions suggested by Crossler *et al.* (2013) are still frequently cited when research is motivated, for example, in research on phishing training (Jampen *et al.*, 2020), information security compliance (Gangire *et al.*, 2021) and information security awareness (Jaeger and Eckhardt, 2021). The suggested directions include how employees can be turned into "security allies," measurements of specific information security behaviors and the adoption of established theories related to culture. This paper follows these three directions and studies the effect of a training program on multiple types of information security behaviors as indicators of information security culture.

Research on how employees can be turned into "security allies" is often done by studying how training efforts influence behavior through security education, training and awareness (SETA) activities (Hu *et al.*, 2022). Implementing SETA activities is costly, and the literature is dominated by observational studies of SETA and tests of minimal SETA activities. For example, Alshaikh *et al.* (2021) interviewed security managers concerning their views, Chen *et al.* (2015) asked participants about their organizations' SETA efforts, and Jensen *et al.* (2017) conducted an experiment with phishing training using text or figures to be looked at for a few minutes. However, SETA studies have rarely used experimental designs, and when they have, they tend to lack control groups or randomization procedures (Prümmer *et al.*, 2023; Sommestad and Karlzén, 2019). As argued by Shadish *et al.* (2002), this makes causal inference difficult. Furthermore, interventions in most studies target only employees, while

intervention research indicates that interventions are more effective when they target more than one function, for example, both employees and managers (Dyreborg *et al.*, 2022). To address this, the present study reports on a randomized controlled trial of a SETA activity in which employees receive awareness-raising activities and managers receive managerial behavioral training.

The measurement of specific information security behaviors is difficult and costly, both because it requires fieldwork and because of problems associated with privacy and confidentiality. Most published research on compliance information security behavior is therefore limited to self-assessments of intentions to behave in different ways, for example, using questionnaires to ask respondents whether they follow security rules (Cram *et al.*, 2019). The link between self-assessments and actual behavior is often weak; for example, there is a low correlation between the intention to resist phishing emails and the actual behavior of resisting phishing emails (Rocha Flores *et al.*, 2015). Studies of phishing often involve field experiments and measures of actual behaviors; however, the results are often insignificant or mixed (Sommestad and Karlzén, 2019). To address this, the present study includes self-assessments, assessments of colleagues' and managers' behaviors and approaches to information security (i.e. information security leadership and climate; e.g. Gwebu and Wang, 2024), as well as measures of actual behavior.

Behavior does not arise in a vacuum, but is formed in a broader context of environmental contingencies (Sugai *et al.*, 2012). Behavioral choices can be personal or relate to the cultural context of the person performing a behavior. In cultures, behaviors are formed within a social context of shared beliefs, values and norms. Any effort to change a behavior in a group can target the behavior directly, or indirectly via the shared beliefs, values and norms. Additionally, efforts to change behaviors can also affect more abstract approaches and beliefs. It may also be that attempts to change a behavior first results in changes at the cultural level (e.g. leadership), and need more time to spread throughout the culture and later manifest as change in employee behavior. Theories related to information security culture are diverse and address different contexts, such as groups, organizations, industries and countries (Karlsson *et al.*, 2015). Informational security culture has been defined as a shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security (Karlsson *et al.*, 2015). Cultural shared patterns can have a profound impact on what happens in organizations and thus on information security. Information security culture can potentially be developed through shared information security behavioral-learning experiences (Grill, 2018). Interventions that target an organization's information security culture can change employees' and managers' information security behaviors by providing them with collective information security behavioral-learning experiences (Choudhry, 2014). Because the intervention of this study targets both employees and managers, it is expected to produce shared behavioral-learning experiences enabling improvements in the information security culture. The effects should be expected to take a while to materialize at the behavioral level. For instance, conducting effective managerial behavioral training can take months (Grill *et al.*, 2023), and any behavioral change in managerial leadership caused by it need to be experienced by employees to influence their information security behaviors. A longitudinal field experiment spanning 16 months was therefore used in this study. Longitudinal studies of information security behaviors have not been found in the literature. For example, a longitudinal study by Bélanger *et al.* (2022) lasted 10 months but involved no intervention and thus no randomized controlled trial. A trial by Warkentin *et al.* (2016) monitored software use over nine weeks but involved no control group. Yet, randomized controlled trials are needed to establish causal relationships between an intervention and its outcomes (Martin *et al.*, 2021).

The aim of this study was to test the long-term impact of a behavioral training program called Training for Improved Information Security Culture (TIISC) on multiple types of information security behaviors and approaches as indicators of the information security culture. Section 2 describes the theoretical background of this study and related work. Section 3 details the method and TIISC. Section 4 presents the results. Section 5 discusses the implications of these results for research and practice, as well as the limitations of the study. Section 6 concludes the paper.

2. Background and related works

Among practitioners, it is widely recognized that organizational interventions that involve both employees and managers produce better effects. Research on organizational change support the inclusion of both employees and managers. Phillips and Klein (2023) surveyed the practices of change managers and found the following effective strategies: ask for support from senior leadership, ask managers for feedback, listen to managers' concerns, ask employees for feedback and listen to employees' concerns. These general ideas on how to succeed with organizational cultural change are also recognized in the information security literature. For instance, Hu *et al.* (2022) found that the most important factor influencing the success of SETA activities was senior managerial support. Accordingly, the training program tested here targets both managers and employees to produce organizational change in information security culture. Section 2.1 outlines the concepts of information security culture and information security leadership and how they relate to the study described herein. Section 2.2 describes the related work of overall SETA efforts. Section 2.3 describes theory and research on the topic of behavioral leadership training. Section 2.4 describes the training program tested in this study.

2.1 Information security culture, climate and leadership

Culture has been succinctly defined as "the collective programming of the mind that distinguishes the members of one group or category of people from another" (Hofstede, 2011). This definition was part of work on both organizational culture and national culture. In earlier work, Hofstede (1998) explains that "Essential to this definition is that an organization's culture is assumed to reside in the minds of all the organization's members, not only in the minds of its managers or chief executives. Information about an organization's culture should therefore be collected from samples of all these members." Another well-established treatise of organizational culture is due to Schein (1985), who defines culture as a group's "accumulated shared learning", which is a "pattern or system of beliefs, values, and behavioral norms that come to be taken for granted as basic assumptions and eventually drop out of awareness." A related concept to organizational culture is organizational climate. Organizational climate is a reflection of culture and is defined as observable practices, routines and behaviors (Reichers, 1990). This is also similar to the view of culture in Deal and Kennedy (1982) as "the way things are done around here"; that is, how the people in an organization behave in common and predictable ways. In other words, there are similarities and overlaps between the concepts of culture, climate and behavior. However, climate is distinct from culture in that it constitutes the shared perceptions of the manifestation of culture. These manifestations come at different levels of abstraction, such as behaviors, approaches and expressed beliefs.

There are a considerable number of theories on how culture and climate within organizations and societies influence information system development, adoption, use, outcomes and management (Leidner and Kayworth, 2006). Culture has also been explicitly investigated in information security contexts in a number of theoretical and empirical

studies. In such work, the concept of information security culture is used. Karlsson *et al.* (2015) state that "there seems to be a common understanding that it [information security culture] consists of a shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security" (p. 247).

It is widely adopted that information security culture pertains to multiple dimensions related to information security (e.g. values, mental models and activities) within a group. Similarly, in a review of scales for measuring information security culture, Orehek and Petrič (2021) found that most scales are multi-dimensional. Orehek and Petrič elaborated on the "complexity and inclusivity of the concept of information security culture" and concluded that no available scale meets all criteria used in their systematic review. Additionally, the concept of organizational climate has been studied with regards to information security culture, to form information security climate, which is also considered a multidimensional concept (Chan *et al.*, 2005; Gwebu and Wang, 2024; Gyllensten *et al.*, 2022; Gyllensten *et al.*, 2023).

Much information security research has focused on how perceptions of behavioral norms within organizations influence their culture. Most of these studies focus on the behavioral norms of peers and superiors. For example, Herath and Rao (2009) included top management, the boss and colleagues; Siponen *et al.* (2010) included top management, immediate supervisors and peers. The perceived behavioral norms formed by such persons have a substantial impact on intentions to behave securely. For example, a review by Sommestad *et al.* (2019) found that the mean effect correlation between behavioral norms and intentions to behave securely or comply with policies was 0.46. Apart from this focus in information security research on employee policy compliance, there has also been research on employee participation. For instance, Guhr *et al.* (2019) studied intentions of employees in terms of *Information security compliance* and *Information security participation*. In their study, they saw higher levels of compliance and participation among employees with more transformational managers, that is, managers demonstrating higher levels of idealized influence, inspirational motivation, intellectual stimulation and individualized consideration.

Pousette and Törner's (2017) conceptualized information security climate with seven dimensions. Of these, four dimensions concerned the workgroup: *Workgroup commitment to information security*, *Workgroup information security learning*, *Legitimacy of information security rules in the workgroup*, and *Workgroup awareness of information security threats*. The other three dimensions concerned the management: *Management's information security priority*, *Participative information security management*, and *Non-blaming information security management*. Indeed, managers are often identified as being of central importance for how organizational cultures are created and changed (Schein, 1985); for example Krapfl and Kruja (2018) conclude that cultures are more influenced by the leader than by any other single factor. Indeed, information security leadership research describes the importance of leadership for information security performance and have found high cross-sectional correlations between managers' leadership behaviors and employees' information security behaviors (Dang-Pham *et al.*, 2022; Guhr *et al.*, 2019; Rocha Flores and Ekstedt, 2016; Sharma and Aparicio, 2022). Leadership research has studied goal setting, performance feedback, as well as antecedent and consequential leadership (Brand *et al.*, 2020; Gowen, 1985; Gravina *et al.*, 2017; Grill *et al.*, 2023, 2024; Komaki, 1998; Sims, 1977). *Goal setting* represents an antecedent leadership behavior in which managers inform employees of desired future performance (Choi and Johnson, 2022). *Performance feedback* constitutes a consequential leadership behavior in which managers provide employees with information about their behavior, enabling them to adjust future actions (Sleiman *et al.*, 2020). *Antecedent listening* activates participative behaviors among employees, such as inviting

employees to participate in handling information security issues, whereas *Consequential listening* reinforces participative behaviors among employees, such as using employees' input to improve information security management (Grill *et al.*, 2023). Safety leadership research has demonstrated the importance of goal setting, performance feedback, antecedent listening and consequential listening for safety performance (Grill *et al.*, 2023).

In summary, the concept of culture is multidimensional, and has similarities and overlaps with the concepts of climate and behavior. TIISC, the intervention of this study, targets employee behaviors in relation to compliance and participation, as well as the susceptibility to phishing emails. TIISC also targets the more abstract climate approaches concerning employee commitment, learning, awareness and perceived rule legitimacy. In addition, TIISC targets managers' behaviors and approaches to information security. This includes behaviors relating to goal setting, performance feedback as well as antecedent and consequential listening. This also includes the more abstract climate approaches concerning information security priority, participative information security management and non-blaming information security management. Thus, TIISC covers both employees and managers and is designed to produce a positive transfer both between peers in a workgroup and between peers and management.

2.2 Security education training and awareness activities for employees

It is common practice to invest resources in improving peoples' security knowledge and awareness. This is also something typically endorsed by authorities. For example, since 2012, the EU has promoted awareness-raising activities during the European Cybersecurity Month (October) and the US government has held its National Cyber Security Awareness Month (October) since 2004. SETA activities can cover many different topics and be delivered in many ways, and it is not uncommon to develop programs involving multiple activities. This section will give an overview of practice and research concerning the content and delivery method of SETA activity.

When it comes to content, there is no universal standard as to what SETA efforts should cover. For example, National Institute of Standards and Technology (NIST) guidance (Wilson and Hash, 2003) provides a list of 27 examples, including password usage and management, policy, social engineering, unknown e-mail/attachments and shoulder surfing. ENISA (2010) explains that organizations should think carefully by the topics to be covered and provide the examples "lock computer password", "protect equipment and data security" and "surfing the net". The foci of studies related to employee training also vary considerably. The focus of the European Cybersecurity Month was phishing and ransomware in 2022 and social engineering in 2023. The US National Cyber Security Awareness Month in 2023 had the theme "Secure Our World" and recommended four actions: use strong passwords; turn on multi-factor authentication; recognize and report phishing; and update software. Prümmer *et al.* (2023) reviewed 142 papers on security training, finding that the training studied addressed matters ranging from general security concepts to concrete issues such as phishing. It has been suggested that topics should be decided based on the needs of the target audience, the knowledge level of the target audience, real-world examples and the security policies in their organization (Hu *et al.*, 2022).

SETA delivery methods efforts vary, and there is no clear best practice for how material or information should be communicated. NIST (Wilson and Hash, 2003) suggested 17 different ways, including instructor-led sessions, videotapes and mascots. Prümmer *et al.* (2023) also found large variation, in that research studies have investigated and classified training delivery methods as game based, presentation based, simulation based, text based, video based, kinesthetic, visual, aural, reading/writing, knowledge-map based, browser

based, hypermedia, multimedia, hypertext, information based and discussion based. Another classification made by Chowdhury *et al.* (2022) includes conventional methods as well as online and software-based, game-based, video-based, simulation and virtualization-based methods. They also described the advantages and disadvantages of the various methods; for example, conventional methods such as classroom training are said to have the advantage of easily conveying multiple messages at once, but are costly. Hu *et al.* (2022) reported that game-based or hands-on delivery methods have been shown to be more effective than other methods.

TIISC targets the information security culture of workgroups in terms of employees' information security behaviors and attitudes. The effects of SETA activities on such outcomes have been demonstrated in previous research; a concrete example was presented by Hu *et al.* (2022), who found that the perceived criticality of a SETA activity predicts intentions to comply with policy and perform extra-role behaviors (e.g. volunteer for security efforts). The mean effect size of SETA activities on intentions to comply with security policies is medium (d = 0.48; Cram *et al.*, 2019). SETA activities targeting more specific behaviors have also been successful; for example, meta-analyses suggest that anti-phishing training reduces click rates by half (Sommestad and Karlzén, 2019) and reduces susceptibility by 0.85 standard deviations (Baki and Verma, 2023). For instance, Hull *et al.* (2023) showed participants simple infographics and found improvements in phishing detection ability, and Hillman *et al.* (2023) demonstrated learning outcomes by exposing employees to simulated phishing emails in their work environment.

2.3 Behavioral leadership training for managers

Managerial leadership is an important component of organizational culture (Schwatka *et al.*, 2019) and consequently for the success of SETA programs (Hu *et al.*, 2022). In Guhr *et al.*'s (2019) cross-sectional study, transformational leadership behaviors were found to predict both compliance intentions and intentions to participate in information security efforts and in Grill *et al.*'s (2023) randomized controlled trial, performance feedback, antecedent listening and consequential listening were found to constitute fundamental behaviors for transformational leadership. However, research on how to train managers in relevant information security leadership behaviors to become better information security leaders is still lacking. Experience from related fields indicates that behavioral leadership training can improve outcomes that are similar to security, such as safety (Gravina *et al.*, 2019). This section will accordingly present behavioral leadership training theory.

The learning mechanism in behavioral training consists of bringing performers into contact with existing natural sources of reinforcement, such as instrumental and social reinforcement (Choi and Johnson, 2022; Greer, 2020). Effective components of behavioral training are behavior analysis, goal setting, instruction, practice with performance feedback and homework (Choi and Johnson, 2022). Grill *et al.* (2024) showed how leader effectiveness and employee engagement can be improved using these five components when training managers in goal setting, performance feedback and consequential listening. *Behavior analysis* consists of identifying behavioral deficits and excesses and environmental causes of these behavioral issues (Austin *et al.*, 1999). It is usually done by asking relevant informants structured questions about the frequency and duration of a targeted behavior, and about situations in which the behavior is reinforced or punished (Wilder *et al.*, 2018). Assessments by the manager's employees are useful when assessing the frequency and duration of targeted behaviors, while the manager and the trainer can identify situations in which the targeted behavior is reinforced or punished (Grill *et al.*, 2024). *Goal setting* consists of articulating behavioral goals for the training (Brown and Latham, 2002) and

instruction entails providing the manager with information about how and why specific leadership behaviors can be performed. *Practice with performance feedback* involves behavioral rehearsal with a trainer who provides continuous feedback and *homework* entails applying the trained behavior in the manager's everyday work environment. Homework ensures that the behavior is shaped to fit the manager's natural environment and may account for approximately half of the learning effect in behavioral interventions (Kazantzis *et al.*, 2010). Based on these research findings, we designed the information security leadership training method of TIISC described in Section 2.4.

2.4 The training program: Training for Improved Information Security Culture

The training program tested in this research is called TIISC and have two components: employee training and leadership training. These are described below.

The employee training was conducted by one or two information security experts in one video meeting of 2–2.5 h. Each training session started with a brief introduction to information security culture and a short video on a fictional but realistic social engineering attempt. This was followed by several thematic presentations, each introduced with a short lecture, followed by a discussion.

The first theme concerned information security risks at work, in terms of both attacker objectives and attack vectors (relating to video meetings, bring-your-own-device and scam calls). This information was based on well-publicized incidents. The second theme concerned information security rules (e.g. their types and objectives), compliance factors (e.g. the theory of planned behavior), as well as workarounds, trade-offs and deviations from expected behavior. This information was based on the paper by Sommestad *et al*. (2015). The third theme concerned phishing, its prevalence and efficacy, factors explaining its efficacy, as well as protective measures against phishing. This information was based on the meta-analysis by Sommestad and Karlzén (2019). The phishing theme also included having the participants answer a quiz on phishingquiz.withgoogle.com.

The information security leadership training was conducted by an organizational behavior psychologist in accordance with the managerial behavioral training manual (MBT) (Björnsdotter and Grill, 2021; Grill *et al.*, 2024) and comprised six bi-weekly 90-min one-on-one face-to-face individualized training sessions. In these sessions, the managers received individualized training i*n Information security goal setting*, *Information security performance feedback*, *Information security antecedent listening* and *Information security consequential listening*. The training was individualized to the needs and goals of each manager and involved the behavioral training components of behavior analysis, goal setting, instruction, practice with performance feedback and homework. The following section outlines how the MBT was applied to information security leadership training for the participating managers of this study.

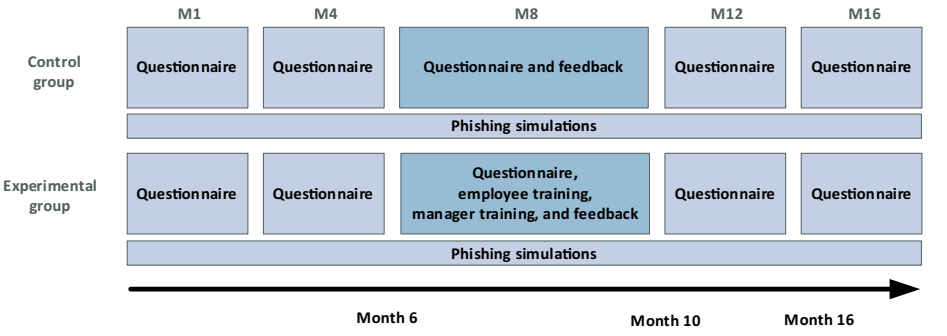
The behavior analysis of the managers' information security leadership behaviors involved a topographic assessment of their pre-intervention levels of *Information security goal setting*, *Information security performance feedback*, *Information security antecedent listening* and *Information security consequential listening*. The behavior analysis was conducted by three parties: the manager's employees, the manager, and the trainer. The employees completed their topographic assessment via questionnaires, while the manager and trainer conducted a joint topographic and functional assessment through a behavioral interview during the two initial training sessions. This behavioral interview included identifying and analyzing the antecedent and consequent stimuli functionally related to the targeted leadership behaviors (i.e. functional analysis; Hanley *et al.*, 2003). During the

behavior analysis, the managers were simultaneously trained to conduct functional analyses of their own leadership behaviors and of functionally related employee behaviors.

Through the behavior analysis, the manager and trainer together identified the manager's most important behavioral deficits in their information security leadership, setting one or two behavioral goals to address these deficits. The goals were mutually agreed on, specified and documented (e.g. "I will formulate and follow up on useful information security goals and procedures together with my employees in our work on developing a documentation strategy for handling project information, including personal data, blueprints, maps, and measurement information"). Instructions were provided to the manager on why and how to conduct behavior analyses of information security behaviors, setting behavioral and participative goals for information security behaviors (Ludwig and Geller, 1997), delivering feedback to employees on information security performance, and employing consequential listening as a reinforcing consequence to employees' information security behaviors (e.g., by validating employee suggestions for improvements in information security management). Practice with performance feedback involved in-session behavioral rehearsal of information security leadership behaviors outlined in the manager's behavioral goals, with managers being recorded during rehearsal and given video feedback (e.g., learning how to organize participative information security meetings with employees). Homework assignments were formulated and written down at the conclusion of each session to ensure that trained information security leadership behaviors were adapted to the manager's work environment (e.g., "On Tuesday, I will carry out participative information-security risk analyses with my employees and my chief information security officers"). These assignments required managers to apply the trained information security leadership behaviors in their work settings. Each assignment was followed up on at the beginning of the subsequent training session, and the managers received performance feedback on all information security leadership behaviors aligned with their goals, informing them of their progress toward achieving those goals.

3. Research methodology

This section describes the participants and procedure, outcome variables and data analysis. Figure 1 illustrates the overall study design, with measurements and durations of each phase. As can be seen, the control group did not receive any training, all groups responded to five questionnaires throughout the study, and all groups' security behavior were measured with



Source(s): Created by the authors

Figure 1. Overall study design, with data collection methods and durations for each phase

simulated phishing emails throughout the study. The sections below describe the sample, ethical clearance, outcome variables and data analysis methods.

3.1 Sample

This study was conducted by involving employees of Swedish organizations in societally important sectors. The Swedish Civil Contingencies Agency, which sponsored the research, considers the following sectors to meet that requirement: energy, food, transport, health-care services, financial services, electronic communications, and services related to safety or security. Public registries were used to produce a list of Swedish organizations providing such services. The organizations in the list were prioritized based on the extent to which their operations concentrated on the relevant sectors, and on whether contact information for the employees in charge of information security could be found. Because of the long duration of the study, organizational stability was sought and only organizations with more than 100 employees were considered. Most contacted organizations declined participation, often because of the invasiveness of measurements, confidentiality, issues related to the ongoing COVID-19 pandemic, or the lengthy study period.

After eight months of recruitment, ten workgroups agreed to participate in the study. In total, 100 employees from seven workgroups were randomly assigned to the experimental condition and 41 employees from three workgroups were randomly assigned to the control condition. Each workgroup had one manager. The employees and managers in the experimental condition received TIISC and feedback on questionnaire ratings, while the employees and managers in the control condition only received feedback on questionnaire ratings. One workgroup in the experimental condition, consisting of two employees, discontinued participation in the study and was consequently excluded from the analyses.

3.2 Ethical clearance

This research was approved by the Swedish Ethical Review Authority (SERA). Informed consent was obtained from the participants, who were informed that they could withdraw their consent at any time and for any reason. The research followed all applicable laws, including Swedish laws on ethical review, freedom of information and secrecy, and the EU General Data Protection Regulation. The informed consent was limited by informing the participants that their computer use was being measured, but not specifically that the measurement involved phishing emails. This limitation of informed consent was implemented for scientifically sound methodological reasons, because the participants' behavior might change if they knew how they were being observed. This study design was also approved by the employers, and the limited informed consent was approved by SERA.

3.3 The outcome variables

The study measured one outcome variable by observing behavior by exposing the employees to simulated phishing emails and recording how these emails were handled. All other outcomes were measured using online questionnaires distributed to the employees at five time points four months apart (see Figure 1). In total, 79 of the employees in the experimental condition (response rate = 81%) and 29 employees in the control condition (response rate = 71%) responded to the questionnaire at one or more time points and were hence included in the data analysis.

3.3.1 Information security employee behaviors and approaches. We directly observed information security behavior in terms of *Phishing susceptibility*, based on simulated emails sent to most employees (67 in the experimental condition and 28 in the control condition) during the study period and measured whether the employees interacted with the emails. The

employees were sent a new phishing email every 8–25 days throughout the study period; in total, 2,294 emails were sent. All emails were variations constructed from 47 templates with different themes, for example, missed invoices and antivirus warnings. The emails either asked the recipient to download and execute a file (n = 1854), execute an attached file (n = 341), or just click a link (n = 95). The templates and their delivery orders were randomly assigned to each recipient. An example of the emails is provided in Appendix 1, Table A1. Each email was associated with a unique web link and a unique executable that made it possible to measure interaction with the email using a web server to which requests were made. A control procedure ensured the reliable delivery of emails and removal of requests made by link scanners and other security systems. The proportion of emails that the recipients interacted with, by clicking or executing, was used as a measure of their *Phishing susceptibility.*

Self-rated information security behaviors were measured by adopting Neal and Griffin's (2006) safety behavior scales, and simply replacing "safety" with "information security." *Information security compliance* was measured using three items (Cronbach's α = 0.86) and *Information security participation* was measured using three items (α = 0.68). The items and response options are detailed in Appendix 1, Table A2.

Employees' information security approaches were measured by asking employees to rate the information security approaches of their colleagues in the workgroup – that is, how information security was generally handled. The Information Security Climate Questionnaire (INSECQ; based on Pousette and Törner, 2017) was used to measure *Workgroup commitment to information security* (four items; α = 0.85), *Workgroup information security learning* (four items; α = 0.77), *Legitimacy of information security rules in the workgroup* (four items; α = 0.82), and *Workgroup awareness of information security threats* (four items; α = 0.63). These climate scales measure approaches that are sometimes akin to behaviors (e.g., "If someone in this workgroup points out a weakness in information security, we try to find a solution") and sometimes closer to beliefs (e.g., "This workgroup believes that the best way to achieve high information security is through clear information security rules"). The items and response options are detailed in Appendix 1, Table A3.

There are reasons to expect that TIISC (i.e., the training program) will have an impact on these measurements. The employee training theme concerning information security risks at work is intended to raise *Workgroup awareness of information security threats*. The theme concerning information security rules is supposed to increase *Information security compliance*, *Workgroup commitment to information security*, and *Legitimacy of information security rules in the workgroup*. The theme concerning phishing may directly lower *Phishing susceptibility.* Additionally, because the training is delivered as a group activity, it may stimulate group activities and changes i*n Information security participation* and *Workgroup information security learning.* Finally, it is also possible that the training of managers will lead to secondary effects on employees, in terms of employee behavior and approaches as described in this section.

3.3.2 Information security leadership behaviors and approaches. The Information Security Leadership Questionnaire (ISLQ) was designed to ask employees about the specific information security leadership behaviors that were targeted in TIISC. Validated leadership scales were adapted to information security leadership by specifying for each item that it asked for the employees' perception of their manager's behavior in handling information security issues. For example, the item "Sets clear organizational goals" of Sjöberg and Grill (2024) was reformulated to "Sets clear information security goals" in ISLQ. *Information security goal setting* was measured using three items (α = 0.97) adapted from the work of Sjöberg and Grill (2024). *Information security performance feedback* was measured using

five items (α = 0.83) adapted from the Safety-Specific and Behavior-specific Feedback Scales of Grill *et al.* (2023), supplemented with one item from the Planning Scale of Sjöberg and Grill (2024). *Information security antecedent listening* was measured using a four-item scale (α = 0.92) adapted from Grill *et al.* (2023). *Information security consequential listening* was measured using a four-item scale (α = 0.86) adapted from the Participative Decision-Making Scale of Arnold *et al.* (2000). The items and response options are detailed in Appendix 2, Table A4.

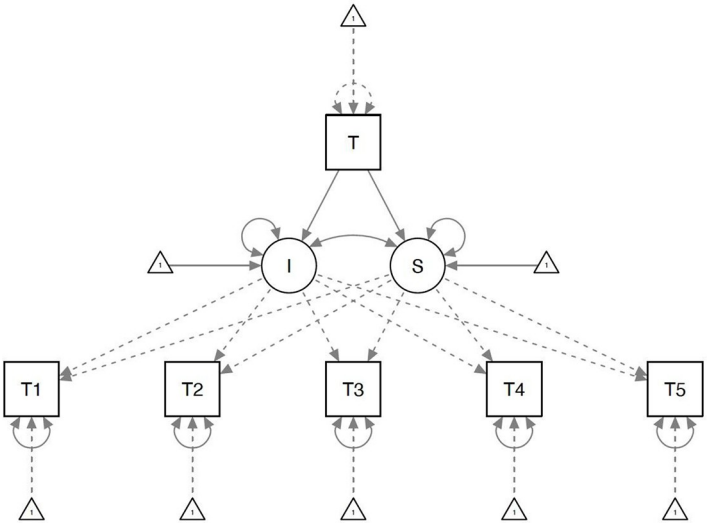
In addition, the Information Security Climate Questionnaire (INSECQ; based on Pousette and Törner, 2017) was used to ask employees about the information security leadership approaches of their managers and supervisors in terms of *Management's information security priority* (four items; α = 0.67), *Participative Information Security Management* (three items; α = 0.52), and *Non-blaming information security management* (four items; α = 0.71). The items and response options are detailed in Appendix 2, Table A5.

There are reasons to expect that TIICS will have an impact on these measurements of behaviors and approaches, as the measurements fit well with the training program. The leadership training is aimed at changing managers' *Information security goal setting*, *Information security performance feedback*, *Information security antecedent listening*, and *Information security consequential listening*. An increase in such leadership behaviors may also lead to changes in the managers' approaches in terms of *Management's information security priority*, *Participative information security management*, and *Non-blaming information security management*.

3.4 Data analysis

Latent growth modeling (LGM) (Duncan *et al.*, 2013; Weinert *et al.*, 2022) was used to assess how TIISC influenced the employees and managers over time. A sample size of at least 100 is preferred for LGM (Curran *et al.*, 2010). LGM is an extension of structural equation modeling (SEM) and involve identifying an appropriate growth curve that describes the development over time in outcome variables and enables the assessment of predictor variables that may control the pattern of growth. See Figure 2 for an illustration of the LGM of this study. In our case, we assessed the extent to which the dichotomous predictor variable of TIISC (labeled T in the figure and taking the value of 0 for the control group and 1 for the experimental group) exerted control over the time-bound change in behaviors and approaches. One growth curve – including the TIISC dichotomous variable – was modeled for each behavior or approach, to assess the difference between the experimental group and the control group in how that behavior or approach developed during the 16-month period. Apart from a latent growth variable (i.e., "S" in Figure 2), LGMs also provide a latent intercept variable (i.e., "I" in Figure 2), that specifies the estimated starting point of each behavior or approach. A randomization check was performed by comparing the latent intercept variable (i.e., the estimated starting value) of each outcome variable in the experimental versus control group – that is, the effect of the TIISC variable on the latent intercept.

Phishing susceptibility behaviors were separated into four periods: T1–T2 = period 1, T2–T3 = period 2, T3–T4 = period 3, and T4–T5 = period 4. For all other outcome variables, mean-level indexes were created for each time point, T1–T5. The factor loadings for the latent slope variable were fixed to zero for T1, one for T2, two for T3, three for T4 and four for T5; this constraint implies that the parameters estimated are equivalent to the average change in the outcome variable between each time point. LGMs were estimated using the software R (version 2023.03.1) with the Lavaan package (version 0.6.14; Rosseel, 2012) applying robust maximum likelihood estimation. In longitudinal research, participants drop in and out, which results in partial missing data; LGM allows for robust maximum likelihood



Note(s): T = TIISC; I = intercept of behavior; S = slope of behavior; T1–T5 = behavior on the first (T1); second (T2); third (T3); fourth (T4); and fifth (T5) measurement occasions
Source(s): Created by the authors

Figure 2. Latent growth model of the influence of TIISC on the change in information security culture variables

estimation, ensuring that all information is used in the models and providing more representative parameter estimates (Yuan and Bentler, 2000).

4. Results

4.1 Demographic and descriptive data

The average age of the employees in the study was 46 years (SD = 11); 59% were female and their average tenure was 11 years (SD = 12). Their managers were on average 47 years (SD = 10); 62% were female and their average tenure was 17 years (SD = 12). Means and standard deviation of the outcome variables at each timepoint are reported in Table 1.

4.2 Latent growth models

The LGM results are reported in Table 2. All but two models converged and showed acceptable goodness-of-fit, implying that the models were appropriate representations of the data (for *Workgroup commitment to information security* and *Workgroup awareness of information security threats*, the slopes displayed negative variance, so no LGM could be estimated for these two outcomes). As evident in the columns for "TIISC on intercept," randomization was successful for all outcome variables except *Information security participation*, which had a higher starting value among employees in the experimental condition ($\beta = 0.32$, $p = 0.01$).

The columns labeled "TIISC on slope" show how TIISC influenced the change in outcome variables over the course of the study period. For employees' information security behaviors and approaches, TIISC was only found to affect the change in *Workgroup*

Table 1. Descriptive statistics (*M* and *SD*) of the outcome variables

Variable	Intervention group		Control group	
	M	*SD*	*M*	*SD*
Phishing susceptibility period 1	0.076	0.112	0.103	0.142
Phishing susceptibility period 2	0.038	0.083	0.044	0.097
Phishing susceptibility period 3	0.046	0.094	0.079	0.139
Phishing susceptibility period 4	0.062	0.131	0.049	0.099
Information security compliance T1	6.21	0.91	6.38	0.67
Information security compliance T2	6.19	0.86	6.41	0.74
Information security compliance T3	6.19	0.94	6.29	0.91
Information security compliance T4	6.11	0.91	6.26	1.04
Information security compliance T5	6.08	0.90	6.21	1.12
Information security participation T1	5.23	1.03	4.51	1.19
Information security participation T2	5.10	1.13	4.48	1.32
Information security participation T3	5.13	1.17	4.00	1.61
Information security participation T4	5.14	1.08	4.43	1.22
Information security participation T5	5.08	1.06	4.27	1.09
Workgroup information security learning T1	4.36	0.85	4.69	0.77
Workgroup information security learning T2	4.60	0.91	4.35	0.94
Workgroup information security learning T3	4.55	0.79	4.33	0.77
Workgroup information security learning T4	4.63	0.85	4.34	0.82
Workgroup information security learning T5	4.59	0.83	4.41	1.12
Legitimacy of information security rules in the workgroup T1	4.75	0.85	4.91	0.78
Legitimacy of information security rules in the workgroup T2	4.70	0.93	4.73	0.63
Legitimacy of information security rules in the workgroup T3	4.61	0.92	4.68	0.83
Legitimacy of information security rules in the workgroup T4	4.63	0.88	4.48	0.84
Legitimacy of information security rules in the workgroup T5	4.67	0.94	5.03	0.76
Information security goal setting T1	4.37	1.61	4.78	1.29
Information security goal setting T2	4.50	1.54	4.16	1.69
Information security goal setting T3	4.35	1.66	4.31	1.61
Information security goal setting T4	4.59	1.49	3.71	1.67
Information security goal setting T5	4.46	1.29	4.42	1.91
Information security antecedent listening T1	3.63	1.40	3.86	1.63
Information security antecedent listening T2	4.15	1.44	3.68	1.41
Information security antecedent listening T3	4.11	1.53	3.37	1.03
Information security antecedent listening T4	4.04	1.51	3.54	1.68
Information security antecedent listening T5	4.22	1.27	3.50	1.76
Information security consequential listening T1	4.72	1.20	5.08	1.20
Information security consequential listening T2	5.09	1.05	4.71	1.05
Information security consequential listening T3	5.00	1.16	4.95	1.16
Information security consequential listening T4	4.99	1.20	4.53	1.20
Information security consequential listening T5	5.21	0.94	4.54	0.94
Information security performance feedback T1	4.87	1.33	5.32	1.20
Information security performance feedback T2	5.18	1.14	5.12	1.05
Information security performance feedback T3	4.92	1.25	5.18	1.16
Information security performance feedback T4	5.21	1.18	4.48	1.20
Information security performance feedback T5	5.23	1.15	5.10	0.94
Management's information security priority T1	4.81	0.77	4.96	0.91
Management's information security priority T2	4.87	0.88	4.94	0.90
Management's information security priority T3	4.65	0.85	5.09	0.75
Management's information security priority T4	4.88	0.80	4.71	0.84
Management's information security priority T5	4.92	0.73	4.84	1.08
Participative information security management T1	3.70	0.99	3.77	0.90

(*continued*)

Table 1. Continued

Variable	Intervention group		Control group	
	M	*SD*	*M*	*SD*
Participative information security management T2	3.94	1.26	3.69	0.88
Participative information security management T3	3.92	1.00	3.65	1.01
Participative information security management T4	3.92	0.91	3.32	0.96
Participative information security management T5	4.15	0.65	3.51	0.89
Non-blaming information security management T1	4.81	0.71	5.13	0.64
Non-blaming information security management T2	4.99	0.79	4.63	1.06
Non-blaming information security management T3	4.84	1.00	5.05	0.80
Non-blaming information security management T4	4.93	0.73	4.57	1.03
Non-blaming information security management T5	5.02	0.67	4.67	1.43

Source(s): Created by the authors

information security learning with medium-size effects ($\beta = 0.50$, $p = 0.02$), using the criteria for "small," "medium," and "large" of Cohen (1992). No effects were found for the change in *Phishing susceptibility* ($\beta = 0.16$, $p = 0.41$), *Information security compliance* ($\beta = 0.06$, $p = 0.77$), *Information security participation* ($\beta = 0.19$, $p = 0.35$), or *Legitimacy of information security rules in the workgroup* ($\beta = -0.03$, $p = 0.93$). As stated above, models could not be constructed for two outcome variables: *Workgroup commitment to information security* and *Workgroup awareness of information security threats*.

For managers' information security leadership behaviors and approaches, TIISC was found to have a medium effect on the change in *Information security consequential listening* ($\beta = 0.65$, $p < 0.01$), *Information security goal setting* ($\beta = 0.53$, $p = 0.03$), and *Participative information security management* ($\beta = 0.50$, $p < 0.01$), and a small effect on the change in *Information security antecedent listening* ($\beta = 0.36$, $p = 0.02$), *Non-blaming information security management* ($\beta = 0.31$, $p = 0.04$), and *Information security performance feedback* ($\beta = 0.25$, $p = 0.08$; NB, significant only at the 0.1 alpha level). The effect of TIISC on the change in *Management's information security priority* ($\beta = 0.19$, $p = 0.29$) was not significant.

5. Discussion

The sections below present the contribution of the paper (Section 5.1), implications of this study for practice (Section 5.2) and research (Section 5.3), together with the limitations of the study (Section 5.4).

5.1 Contribution of the paper

The contribution of this paper is not the TIISC training program *per se*. This study designed the SETA to include a mixture of video, lectures and discussions in a session of a few hours for the employees; this is typical and uncontroversial. However, this study also targeted managers with leadership training, which is a fairly new idea in the security domain. As described in Section 2.1, the combination of training targeting employees and managers are motivated by theories on information security culture, which TIISC is set to influence. More specifically, theory related to information security culture describe culture as a group phenomenon, where employees' perceptions of norms and incentives are important, and managers' behaviors and approaches related to information security can be a key component

Table 2. LGM results for the influence of TIISC on the change in information security culture variables

	Intercept				Slope				TIISC on intercept				TIISC on slope				Goodness of fit		
Variable	Est.	*SE*	*p*	*β*	Est.	*SE*	*p*	*β*	Est.	*SE*	*p*	*β*	Est.	*SE*	*p*	*β*	χ^2	CFI	RMSEA
Employees' information security behaviors and approaches																			
Phishing susceptibility[a]	0.10	0.02	<0.01	2.90	–0.05	0.02	0.02	–1.94	–0.02	0.02	0.25	–0.34	0.01	0.01	0.41	0.16	6.39	0.97	0.03
Information security compliance	6.45	0.11	<0.01	9.16	–0.05	0.06	0.37	–0.36	–0.20	0.17	0.22	–0.13	0.02	0.06	0.77	0.06	7.77	1.00	0.00
Information security participation	4.50	0.22	<0.01	4.77	–0.07	0.05	0.13	–0.55	0.67	0.56	0.01	0.32	0.06	0.06	0.35	0.19	8.96	1.00	0.00
Workgroup information security learning	4.56	0.15	<0.01	6.46	–0.06	0.05	0.22	–0.52	–0.21	0.18	0.23	–0.13	0.14	0.06	0.02	0.50	12.06	1.00	0.00
Legitimacy of information security rules in the workgroup	4.78	0.13	<0.01	7.35	0.01	0.03	0.80	0.12	–0.10	0.17	0.56	–0.07	–0.00	0.04	0.93	–0.03	12.46	1.00	0.00
Managers' information security leadership behaviors and approaches																			
Information security goal setting	4.48	0.26	<0.01	3.47	–0.11	0.08	0.15	–0.64	–0.18	0.32	0.58	–0.06	0.20	0.09	0.03	0.53	12.27	1.00	0.00
Information security antecedent listening	3.67	0.26	<0.01	3.03	–0.06	0.07	0.42	–0.21	–0.03	0.32	0.93	–0.01	0.22	0.09	0.02	0.36	11.41	1.00	0.00
Information security consequential listening	4.88	0.25	<0.01	5.42	–0.13	0.05	0.02	–0.78	–0.16	0.28	0.57	–0.07	0.25	0.06	<0.01	0.65	11.27	1.00	0.00
Information security performance feedback	5.20	0.25	<0.01	4.65	–0.11	0.09	0.26	–0.31	–0.29	0.30	0.33	–0.11	0.19	0.11	0.08	0.25	16.41	0.98	0.08
Management's information security priority	4.99	0.15	<0.01	8.55	–0.04	0.06	0.48	–0.27	–0.22	0.17	0.22	–0.16	0.07	0.06	0.29	0.19	7.06	1.00	0.00
Participative information security management	3.75	0.16	<0.01	5.19	–0.09	0.04	0.04	–0.55	–0.02	0.20	0.93	–0.01	0.19	0.06	<0.01	0.50	4.62	1.00	0.00
Non-blaming information security management	5.01	0.17	<0.01	7.66	–0.10	0.07	0.15	–0.45	–0.21	0.19	0.27	–0.14	0.16	0.08	0.04	0.31	13.98	1.00	0.00

Note(s): $n = 108$, $df = 13$.[a] The change in phishing susceptibility was curvilinear; that is, it included a quadratic slope of est. = 0.01, $SE = 0.01$, $p = 0.03$, $\beta = 2.37$
Source(s): Created by the authors

of information security culture. Accordingly, TIISC was designed to target both employees and managers in selected workgroups to produce a substantial change within the groups. Hence, the main contribution of this study lies in combining traditional employee training with a novel procedure for information security leadership training, and the test of the combination's efficacy to change the information security culture in workgroups.

The rigor of the evaluation is a key component of this contribution. As noted by Prümmer *et al.* (2023), there is a lack of long-term evaluations of training effects in the security field, and this study evaluates a broad set of outcomes over a long period. In addition, a longitudinal randomized controlled trial provides the highest standards for generalized causal inference (Shadish *et al.*, 2002). The long time period and complicated study design have limited the sample size of the study. However, the results clearly demonstrate that some variables (e.g., employees' information security learning processes and managers' reinforcement of employee participation in information security issues) are improved by a training program such as TIISC. Thus, this approach, targeting multiple levels of a workgroup, appears to have a broad impact on the perceptions and attitudes within workgroups. Furthermore, the rigor and long duration of the study highlight that some changes (e.g. in *Phishing susceptibility*) would have been falsely attributed to the training if a shorter and less complicated study design would have been used. We elaborate further on these findings below.

5.2 Implications for practice

TIISC covered training for both employees and managers. The intention behind TIISC was not to produce something complicated or novel, but to test the effect of an uncontroversial type of employee training combined with managerial leadership training in a controlled manner. The effect sizes for employees' information security behaviors and approaches should therefore be indicative of what typical training programs will produce. As leadership training in information security is a more novel SETA element, less is known about the expected effect sizes of TIISC on information security leadership behaviors and approaches. The results indicate that TIISC had a medium effect on *Workgroup information security learning* as well as medium effects on *Managers' information security goal setting*, *Information security consequential listening*, and *Participative information security management*. TIISC also had small effects on *Managers' information security antecedent listening* and *Non-blaming information security management*. In addition, *Information security performance feedback* was subject to a small effect (but only significant at the alpha-level of <0.1).

The effects on many of the leadership variables indicate that the information security leadership training was successful. Training managers in functional behavior analysis, setting and following up information security goals, involving employees in analyzing and solving information security issues, and providing behavior-specific information security performance feedback can constitute an important component in developing efficient information security leadership and information security culture. Providing managers with individualized training designed to address the individual manager's and their organization's information security issues and goals, enables managers to improve the information security culture in their organizations.

Workgroup information security learning saw the only statistically significant improvement for employee behaviors and approaches. The increase in *Workgroup information security learning* can be interpreted as a result of employee training leading to employees' being more confident and active in suggesting and advocating for solutions to information security problems, as well as in taking each other's solutions seriously. The increase in *Workgroup*

information security learning can also be interpreted as a result of the managers involving their employees in information security management, including setting and following up on information security goals, and collectively designing information security rules and guidelines. It is also possible that these two interpretations should be combined, with the increase in learning being due to the involvement of both employees and managers in the same intervention. Such combinations have been shown to be powerful in the past; for instance, talking about security issues within and across functions in a learning climate is an important way of creating a strong information security culture in organizations (Albrechtsen and Hovden, 2010). The implication for practice is that the two-pronged approach of TIISC may be critical to substantially improve *Workgroup information security learning*.

Overall, TIISC was found to have a more substantial effect on managers' information security leadership behaviors and approaches than on employees' information security behaviors and approaches. This difference may be due to the design of TIISC: the employees received only 2–2.5 h of training via a video meeting, while the managers received six 90-min one-on-one face-to-face sessions, for a total of nine hours. However, the training for employees occupied the time of many more individuals during the sessions, so the total work time spent in TIISC by the employees far exceeded that of the managers. Taking one step back, it is worth noting that the evidence is strong for the relationship between managers' leadership behaviors and employees' performance (Avolio *et al.*, 2009). It is possible that the mostly small or non-significant effect of TIISC on employees' information security behaviors is due to insufficient time-lag between cause and effect (Krause *et al.*, 1999). TIISC was carried out between T2 and T4, implying that the time-lag between completing the intervention and the last measurement was as short as four months for some of the employees. Cultural changes may take considerably longer to materialize, as they require extensive interactions between managers and employees. This would also fit with the employee effect being limited to *Workgroup information security learning*, which reasonably comes before other improvements in employees. The implications for practice are that organizations should not expect quick results when working on improving their information security cultures, and need to carefully consider the division of efforts between training managers and training employees.

Another result of practical relevance concerns the phishing simulations. TIISC did not have a significant influence on *Phishing susceptibility*. However, as the slope of *Phishing susceptibility* reported in Table 1 indicates, there was a large and significant reduction in *Phishing susceptibility* in both the experimental and control groups. In fact, this was the biggest change observed in the study: from the first to second four-month period, *Phishing susceptibility* across the sample had decreased from around 9% to around 5%. We believe that the frequent exposure to phishing emails gave participants an unintended learning opportunity. In retrospect, this is not surprising. While the phishing emails in this study did not expose participants to training materials or pointers, as many phishing training programs do, they gave participants a chance to recognize phishing emails (or at least emails that did not contain actual salary lists, invoices, etc.). The mere exposure to simulated phishing emails appears to have produced a strong tendency to handle phishing emails better in the future. The implication for practice is that even basic exposure of participants to phishing simulations, with no other intervention or support related to phishing, seems to be a good practice to implement.

5.3 Implications for researchers

Crossler *et al.* (2013) outlined directions for research on behavioral information security. They argued that technical solutions are not enough to ensure high information security standards, as the information security behaviors of individuals are the predominant weakness

in most organizations. Interventions designed to improve information security behaviors are therefore a priority for research and practice if we are to achieve sufficient security levels in organizations in societally important sectors.

This study aimed to test the long-term impact of a behavioral training program called TIISC on multiple information security behaviors as indicators of the information security culture. The results indicate that the intervention had significant positive effects on most types of managers' information security leadership behaviors and approaches, but on only one type of employees' information security behavior or approach. Information security interventions targeting managers are difficult to find in the literature. The present results suggest that such interventions may be worthwhile: an intervention consuming fewer than ten hours of each manager's time has a significant positive effect on how the managers lead their employees in matters related to information security. More research in this vein is suggested. Future research could investigate leadership training in isolation or in conjunction with employee training, as done here. With even longer study periods (e.g., 12 months after the intervention), effects on employees' behaviors and approaches may become clearer.

A side result of this study is the large effect of phishing simulations on *Phishing susceptibility*. We believe this finding is critical for future phishing research, as it highlights the importance of the randomized controlled trial: if it were not for the control condition, we could incorrectly have attributed the large decrease in *Phishing susceptibility* to the intervention. The reason why the effect of TIISC on *Phishing susceptibility* was not statistically significantly different between conditions may be that most of the variation in *Phishing susceptibility* was explained by the mere exposure to phishing simulations, leaving TIISC with a very small amount of variation in *Phishing susceptibility* to explain. Sommestad and Karlzén (2019) found that 31 of 48 experiments on *Phishing susceptibility* did not have a control group. It is likely that some of those experiments confused the effect of their interventions with the effect of being exposed to phishing simulations.

5.4 Limitations of the study

This study has some limitations. Recruiting participants to this study was difficult, partly due to the ongoing COVID-19 pandemic. The long study period, and reliance on respondents completing questionnaires, also led to some problems: during the study period, individuals joined and left the studied workgroups. Thus, some employees did not receive the first questionnaires, and some did not receive the last ones. Although the maximum likelihood estimation used is effective in handling partially missing data, there may still have been some selection bias affecting the responses. It is also possible that the results would have been different for employees in organizations in countries other than Sweden.

The small sample size of 108 employees makes generalizations difficult. It is possible that with a bigger sample, more of the outcome variables would have displayed statistically significant changes due to TIISC. Additionally, a larger sample would have made the failed randomization for participative behavior less likely. Insignificant results may also have been partially caused by the suboptimal reliability of some of the scales used: the internal reliabilities of *Information security participation*, *Workgroup awareness of information security threats*, *Management's information security priority*, and *Participative information security management* were below 0.7. This implies that the reliabilities of these measures were unsatisfactory and included substantial measurement error that lowered measurable effects. These scales were adapted from validated scales, but the adaption may have reduced their reliabilities.

There are many other potential explanations for the insignificant effects on *Information security compliance*, *Information security participation*, *Phishing susceptibility*, *Legitimacy of information security rules in the workgroup*, and *Management's information security*

priority. The most obvious one concerns the scope and design of TIISC. Both the research budget and the participants' budget limited how comprehensive the intervention could be. We believe that TIISC is typical of what contemporary organizations in societally important sectors implement themselves. However, both the employee training and leadership training could be more comprehensive, and this would probably result in larger effects. Other factors contributing to the insignificant results are also possible. In particular, participants were recruited to this study from societally important sectors, which, in conjunction with the difficulty of recruiting participants, may have led to selection bias. For instance, organizations that are confident in their security management practices and employ individuals interested in information security may be overrepresented among those that chose, and were chosen, to participate. The participants demonstrated a relatively high level of information security behaviors and approaches before the intervention. As the intercept of Table 2 shows, the mean starting value of the participants' *Information security compliance* was 6.45 on a scale from 1 to 7. The effect on this outcome was thus probably limited by ceiling effects, and interventions in other settings may produce larger effects.

6. Conclusions

By incorporating managerial behavioral training in the design of SETA programs, substantial changes in behaviors and approaches can be accomplished. Specifically, medium effects can be achieved on managers' information security leadership in terms of *Managers' information security goal setting*, *Information security consequential listening*, and *Participative information security management*. These improvements were achieved through behavioral analysis of information security behaviors, goal setting, instruction, practice with performance feedback, and homework. Additionally, a medium effect can be achieved for employees in relation to *Workgroup information security learning*. TIISC is a promising intervention procedure that can contribute to improved information security cultures in organizations responsible for information of societal importance.

References

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers and Security*, Vol. 29 No. 4, pp. 432-445.

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021), "Applying social marketing to evaluate current security education training and awareness programs in organisations", *Computers and Security*, Vol. 100, p. 102090, doi: 10.1016/j.cose.2020.102090.

Arnold, J.A., Arad, S., Rhoades, J.A. and Drasgow, F. (2000), "The empowering leadership questionnaire: the construction and validation of a new scale for measuring leader behaviors", *Journal of Organizational Behavior*, Vol. 21 No. 3, pp. 249-269, doi: 10.1002/(SICI)1099-1379(200005)21:3%3C249::AID-JOB10%3E3.0.CO;2-%23.

Austin, J., Carr, J.E. and Agnew, J.L. (1999), "The need for assessment of maintaining variables in OBM", *Journal of Organizational Behavior Management*, Vol. 19 No. 2, pp. 59-87, doi: 10.1300/J075v19n02_05.

Avolio, B.J., Reichard, R.J., Hannah, S.T., Walumbwa, F.O. and Chan, A. (2009), "A meta-analytic review of leadership impact research: experimental and quasi-experimental studies article", *The Leadership Quarterly*, Vol. 20 No. 5, pp. 764-784, doi: 10.1016/j.leaqua.2009.06.006.

Baki, S. and Verma, R.M. (2023), "Sixteen years of phishing user studies: what have we learned?", *IEEE Transactions on Dependable and Secure Computing*, Vol. 20 No. 2, pp. 1200-1212, doi: 10.1109/TDSC.2022.3151103.

Bélanger, F., Maier, J. and Maier, M. (2022), "A longitudinal study on improving employee information protective knowledge and behaviors", *Computers and Security*, Vol. 116, p. 102641, doi: 10.1016/j.cose.2022.102641.

Björnsdotter, A. and Grill, M. (2021), *Chefshandledning: En Manual till Funktionellt Ledarskap [Managerial Behavioral Training for Functional Leadership]*, Studentlitteratur.

Brand, D., Novak, M.D., DiGennaro Reed, F.D. and Tortolero, S.A. (2020), "Examining the effects of feedback accuracy and timing on skill acquisition", *Journal of Organizational Behavior Management*, Vol. 40 Nos 1/2, pp. 3-18, doi: 10.1080/01608061.2020.1715319.

Brown, T.C. and Latham, G.P. (2002), "The effects of behavioural outcome goals, learning goals, and urging people to do their best on an individual's teamwork behaviour in a group problem-solving task", *Canadian Journal of Behavioural Science / Revue Canadienne Des Sciences du Comportement*, Vol. 34 No. 4, p. 276, doi: 10.1037/h0087180.

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security in the workplace: linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, Vol. 1 No. 3, pp. 18-41.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2015), "Impacts of comprehensive information security programs on information security culture", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19, doi: 10.1080/08874417.2015.11645767.

Choi, E. and Johnson, D.A. (2022), "Common antecedent strategies within organizational behavior management: the use of goal setting, task clarification, and job aids", *Journal of Organizational Behavior Management*, Vol. 42 No. 1, pp. 75-95, doi: 10.1080/01608061.2021.1967834.

Choudhry, R.M. (2014), "Behavior-based safety on construction sites: a case study", *Accident Analysis and Prevention*, Vol. 70, pp. 14-23, doi: 10.1016/j.aap.2014.03.007.

Chowdhury, N., Katsikas, S. and Gkioulos, V. (2022), "Modeling effective cybersecurity training frameworks: a delphi method-based study", *Computers and Security*, Vol. 113, p. 102551, doi: 10.1016/j.cose.2021.102551.

Cohen, J. (1992), "A power primer", *Psychological Bulletin*, Vol. 112 No. 1, pp. 155-159, doi: 10.1037/0033-2909.112.1.155.

Cram, W.A., D'arcy, J. and Proudfoot, J.G. (2019), "Seeing the Forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554, doi: 10.25300/misq/2019/15117.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers and Security*, Vol. 32, pp. 90-101, doi: 10.1016/j.cose.2012.09.010.

Curran, P.J., Obeidat, K. and Losardo, D. (2010), "Twelve frequently asked questions about growth curve modeling", *Journal of Cognition and Development*, Vol. 11 No. 2, pp. 121-136.

Dang-Pham, D., Kautz, K., Hoang, A.-P. and Pittayachawan, S. (2022), "Identifying information security opinion leaders in organizations: insights from the theory of social power bases and social network analysis", *Computers and Security*, Vol. 112, p. 102505, doi: 10.1016/j.cose.2021.102505.

Deal, T.E. and Kennedy, A.A. (1982), "Corporate cultures: the rites and rituals of corporate life", Addison-Wesley Publishing Company, available at: https://books.google.se/books?id=9_L7qnCEiUwC

Duncan, T.E., Duncan, S.C. and Strycker, L.A. (2013), *An Introduction to Latent Variable Growth Curve Modeling: Concepts, Issues, and Application*, Routledge Academic.

Dyreborg, J., Lipscomb, H.J., Nielsen, K., Törner, M., Rasmussen, K., Frydendall, K.B., Bay, H., Gensby, U., Bengtsen, E. and Guldenmund, F. (2022), "Safety interventions for the prevention of accidents at work: a systematic review", *Campbell Systematic Reviews*, Vol. 18 No. 2, p. e1234, doi: 10.1002/cl2.1234.

ENISA (2010), "The new users' guide: how to raise information security awareness".

Gangire, Y., Da Veiga, A. and Herselman, M. (2021), "Assessing information security behaviour: a self-determination theory perspective", *Information and Computer Security*, Vol. 29 No. 4, pp. 625-646.

Gowen, C.R. (1985), "Managing work group performance by individual goals and group goals for an interdependent group task", *Journal of Organizational Behavior Management*, Vol. 7 Nos 3/4, pp. 5-27, doi: 10.1300/J075v07n03_02.

Gravina, N., King, A. and Austin, J. (2017), "Leadership's role in process safety: an understanding of behavioral science among managers and executives is needed", *Journal of Organizational Behavior Management*, Vol. 37 Nos 3/4, pp. 316-331, doi: 10.1080/01608061.2017.1340925.

Gravina, N., King, A. and Austin, J. (2019), "Training leaders to apply behavioral concepts to improve safety", *Safety Science*, Vol. 112, pp. 66-70, doi: 10.1016/j.ssci.2018.10.013.

Greer, R.D. (2020), "The selector in behavior selection", *The Psychological Record*, Vol. 70 No. 4, pp. 543-558, doi: 10.1007/s40732-020-00385-3.

Grill, M. (2018), "Safety leadership in the construction industry: managing safety at *Swedish and Danish construction* sites", Doctoral Thesis. University of Gothenburg, Sahlgrenska Academy, available at: https://gupea.ub.gu.se/handle/2077/53619

Grill, M., Pousette, A. and Björnsdotter, A. (2024), "Managerial behavioral training for functional leadership: a randomized controlled trial", *Journal of Organizational Behavior Management*, Vol. 44 No. 1, pp. 15-41, doi: 10.1080/01608061.2023.2171174.

Grill, M., Ulfdotter Samuelsson, A., Matton, E., Norderfeldt, E., Rapp-Ricciardi, M., Räisänen, C. and Larsman, P. (2023), "Individualized behavior-based safety-leadership training: a randomized controlled trial", *Journal of Safety Research*, Vol. 87, pp. 332-344, doi: 10.1016/j.jsr.2023.08.005.

Guhr, N., Lebek, B. and Breitner, M.H. (2019), "The impact of leadership on employees' intended information security behaviour: an examination of the full-range leadership theory", *Information Systems Journal*, Vol. 29 No. 2, pp. 340-362, doi: 10.1111/isj.12202.

Guo, K.H. (2013), "Security-related behavior in using information systems in the workplace: a review and synthesis", *Computers and Security*, Vol. 32, pp. 242-251, doi: 10.1016/j.cose.2012.10.003.

Gwebu, K.L. and Wang, J. (2024), "The defining features of a robust information security climate", *Computers and Security*, Vol. 142, p. 103891.

Gyllensten, K., Pousette, A. and Törner, M. (2022), "Value conflicts and information security – a mixed-methods study in high-risk industry", *Information and Computer Security*, Vol. 30 No. 3, pp. 346-363.

Gyllensten, K., Törner, M. and Pousette, A. (2023), "The impact of psychosocial working conditions on information security behaviour in the nuclear industry", *Information and Computer Security*, Vol. 31 No. 1, pp. 32-50.

Hanley, G.P., Iwata, B.A. and McCord, B.E. (2003), "Functional analysis of problem behavior: a review", *Journal of Applied Behavior Analysis*, Vol. 36 No. 2, pp. 147-185, doi: 10.1901/jaba.2003.36-147.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Hillman, D., Harel, Y. and Toch, E. (2023), "Evaluating organizational phishing awareness training on an enterprise scale", *Computers and Security*, Vol. 132, doi: 10.1016/j.cose.2023.103364.

Hofstede, G. (1998), "Identifying organizational subcultures: an empirical approach", *Journal of Management Studies*, Vol. 35 No. 1, pp. 1-12.

Hofstede, G. (2011), "Dimensionalizing cultures: the Hofstede model in context", *Online Readings in Psychology and Culture*, Vol. 2 No. 1, p. 8.

Hull, D.M., Schuetz, S.W. and Lowry, P.B. (2023), "Tell me a story: the effects that narratives exert on meaningfulengagement outcomes in antiphishing training", *Computers and Security*, Vol. 129, p. 103252, doi: 10.1016/j.cose.2023.103252.

Hu, S., Hsu, C. and Zhou, Z. (2022), "Security education, training, and awareness programs: literature review", *Journal of Computer Information Systems*, Vol. 62 No. 4, pp. 752-764, doi: 10.1080/08874417.2021.1913671.

Jaeger, L. and Eckhardt, A. (2021), "Eyes wide open: the role of situational information security awareness for security-related behaviour", *Information Systems Journal*, Vol. 31 No. 3, pp. 429-472.

Jampen, D., Gür, G., Sutter, T. and Tellenbach, B. (2020), "Don't click: towards an effective anti-phishing training. A comparative literature review", *Human-Centric Computing and Information Sciences*, Vol. 10 No. 1, p. 33.

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B. (2017), "Training to mitigate phishing attacks using mindfulness techniques", *Journal of Management Information Systems*, Vol. 34 No. 2, pp. 597-626, doi: 10.1080/07421222.2017.1334499.

Karlsson, F., Åström, J. and Karlsson, M. (2015), "Information security culture–state-of-the-art review between 2000 and 2013", *Information and Computer Security*, Vol. 23 No. 3, pp. 246-285, doi: 10.1108/ICS-05-2014-0033.

Kazantzis, N., Whittington, C. and Dattilio, F. (2010), "Meta-analysis of homework effects in cognitive and behavioral therapy: a replication and extension", *Clinical Psychology: Science and Practice*, Vol. 17 No. 2, pp. 144-156, doi: 10.1111/j.1468-2850.2010.01204.x.

Komaki, J.L. (1998), *Leadership from an Operant Perspective*, Routledge.

Krapfl, J.E. and Kruja, B. (2018), "Leadership and culture", *Journal of Organizational Behavior Management*, Vol. 35 Nos 1/2, pp. 28-43, doi: 10.1080/01608061.2015.1031431.

Krause, T.R., Seymour, K. and Sloat, K. (1999), "Long-term evaluation of a behavior-based method for improving safety performance: a meta-analysis of 73 interrupted time-series replications", *Safety Science*, Vol. 32 No. 1, pp. 1-18, doi: 10.1016/S0925-7535(99)00007-7.

Leidner, D.E. and Kayworth, T. (2006), "A review of culture in information systems research: toward a theory of information technology culture conflict", *MIS Quarterly*, Vol. 30 No. 2, pp. 357-399.

Ludwig, T.D. and Geller, E.S. (1997), "Assigned versus participative goal setting and response generalization: managing injury control among professional pizza deliverers", *Journal of Applied Psychology*, Vol. 82 No. 2, p. 253, doi: 10.1037/0021-9010.82.2.253.

Martin, R., Hughes, D.J., Epitropaki, O. and Thomas, G. (2021), "In pursuit of causality in leadership training research: a review and pragmatic recommendations", *The Leadership Quarterly*, Vol. 32 No. 5, p. 101375, doi: 10.1016/j.leaqua.2019.101375.

Neal, A. and Griffin, M.A. (2006), "A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels", *Journal of Applied Psychology*, Vol. 91 No. 4, pp. 946-953, doi: 10.1037/0021-9010.91.4.946.

Orehek, Š. and Petrič, G. (2021), "A systematic review of scales for measuring information security culture", *Information and Computer Security*, Vol. 29 No. 1, pp. 133-158.

Phillips, J. and Klein, J.D. (2023), "Change management: from theory to practice", *TechTrends*, Vol. 67 No. 1, pp. 189-197, doi: 10.1007/s11528-022-00775-0.

Pousette, A. and Törner, M. (2017), "Kunskap om informationssäkerhetsklimat ger verktyg för förändring", in Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B. and Törner, M. (Eds), *Informationssäkerhet Och Organisationskultur [Information Security and Organizational Culture]*, Studentlitteratur.

Prümmer, J., van Steen, T. and van den Berg, B. (2023), "A systematic review of current cybersecurity training methods", *Computers and Security*, Vol. 136, doi: 10.1016/j.cose.2023.103585.

Reichers, A. (1990), *Climate and Culture: An Evolution of Constructs*, Organizational Climate and Culture/Jossey-Bass Publishers.

Rocha Flores, W. and Ekstedt, M. (2016), "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness", *Computers and Security*, Vol. 59, pp. 26-44, doi: 10.1016/j.cose.2016.01.004.

Rocha Flores, W., Holm, H., Nohlberg, M. and Ekstedt, M. (2015), "Investigating personal determinants of phishing and the effect of national culture", *Information and Computer Security*, Vol. 23 No. 2, pp. 178-199, doi: 10.1108/ICS-05-2014-0029.

Rosseel, Y. (2012), "Lavaan: an R package for structural equation modeling", *Journal of Statistical Software*, Vol. 48 No. 2, pp. 1-36, doi: 10.18637/jss.v048.i02.

Schein, E.H. (1985), *Organizational Culture and Leadership*, Jossey-Bass.

Schwatka, N.V., Goldenhar, L.M., Johnson, S.K., Beldon, M.A., Tessler, J., Dennerlein, J.T., Fullen, M. and Trieu, H. (2019), "A training intervention to improve frontline construction leaders' safety leadership practices and overall jobsite safety climate", *Journal of Safety Research*, Vol. 70, pp. 253-262, doi: 10.1016/j.jsr.2019.04.010.

Shadish, W., Cook, T.D. and Campbell, D.T. (2002), *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*, Wadsworth Cengage Learning.

Sharma, S. and Aparicio, E. (2022), "Organizational and team culture as antecedents of protection motivation among IT employees", *Computers and Security*, Vol. 120, p. 102774, doi: 10.1016/j.cose.2022.102774.

Sims, H.P. (1977), "The leader as a manager of reinforcement contingencies: an empirical example and a model", in Hunt, J.G. and Larson, L.L. (Eds), *Leadership: The Cutting Edge*, Southern IL University Press, p. 137.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: an empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71.

Sjöberg, A. and Grill, M. (2024), "A validity study of a work sample test of leadership behavior using supervisor and subordinate ratings as criteria", *Scandinavian Journal of Psychology*, Vol. 65 No. 1, pp. 129-135, doi: 10.1111/sjop.12954.

Sleiman, A.A., Sigurjonsdottir, S., Elnes, A., Gage, N.A. and Gravina, N.E. (2020), "A quantitative review of performance feedback in organizational settings (1998-2018)", *Journal of Organizational Behavior Management*, Vol. 40 Nos 3/4, pp. 303-332, doi: 10.1080/01608061.2020.1823300.

Sommestad, T. and Karlzén, H. (2019), "A meta-analysis of field experiments on phishing susceptibility", *2019 APWG symposium on electronic crime research (eCrime)*, pp. 1-14, doi: 10.1109/eCrime47957.2019.9037502.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security*, Vol. 23 No. 2, pp. 200-217, doi: 10.1108/ICS-04-2014-0025.

Sommestad, T., Karlzén, H. and Hallberg, J. (2019), "The theory of planned behavior and information security policy compliance", *Journal of Computer Information Systems*, Vol. 59 No. 4.

Sugai, G., O'Keeffe, B.V. and Fallon, L.M. (2012), "A contextual consideration of culture and school-wide positive behavior support", *Journal of Positive Behavior Interventions*, Vol. 14 No. 4, pp. 197-208, doi: 10.1177/10983007114263.

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

Weinert, C., Maier, C., Laumer, S. and Weitzel, T. (2022), "Repeated IT interruption: habituation and sensitization of user responses", *Journal of Management Information Systems*, Vol. 39 No. 1, pp. 187-217, doi: 10.1080/07421222.2021.2023411.

Wilson, M. and Hash, J. (2003), "Building an information technology security awareness and training program", *NIST Special Publication*, Vol. 800 No. 50, pp. 1-39, doi: 10.6028/NIST.SP.800-50.

Wilder, D.A., Lipschultz, J.L., King, A., Driscoll, S. and Sigurdsson, S. (2018), "An analysis of the commonality and type of preintervention assessment procedures in the journal of organizational behavior management (2000–2015)", *Journal of Organizational Behavior Management*, Vol. 38 No. 1, pp. 5-17, doi: 10.1080/01608061.2017.1325822.

Yuan, K.-H. and Bentler, P.M. (2000), "Three likelihood-based methods for mean and covariance structure analysis with nonnormal missing data", *Sociological Methodology*, Vol. 30 No. 1, pp. 165-200, doi: 10.1111/0081-1750.00078.

Further reading

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Corresponding author

Martin Grill can be contacted at: martin.grill@gu.se

Appendix 1. Information security employee behaviors and approaches

Table A1. Phishing susceptibility. Example of phishing emails with and without added adaptations and influence techniques

Template	Suspicious user activities 1
From	Customersupport@[retacted domain].se
Subject	Anomalous activity on your computer
Body	Dear John Doe We have discovered anomalous activities on your computer and cannot check this over the network. We need your help to execute a program that sets the configuration for the domain correctly http://downloads.[retacted domain].se/files/kdkws If you do not do this within one week, your computer will be removed from the domain. Thanks in advance, IT-department, ACME enterprises

Source(s): Created by the authors

Table A2. Self-rated information security behaviors

	Information security behavior	Never	Almost never	Rarely	Sometimes	Fairly often	Frequently	Always
1	I use all necessary information security measures in my work	☐	☐	☐	☐	☐	☐	☐
2	I follow all information security regulations in my work	☐	☐	☐	☐	☐	☐	☐
3	I maintain the highest possible level of information security in my work	☐	☐	☐	☐	☐	☐	☐
4	I do what I can to support information security efforts in my workplace	☐	☐	☐	☐	☐	☐	☐
5	I put in extra effort to improve the information security of the workplace	☐	☐	☐	☐	☐	☐	☐
6	I volunteer to take on tasks to help improve information security in my workplace	☐	☐	☐	☐	☐	☐	☐

Note(s): Respondents are asked to "describe your security-related behaviors at work". Items 1–3 measure Information security compliance; items 4–6 measure Information security participation. All items are based on the work of Neal and Griffin (2006) and adapted to the information security context
Source(s): Created by the authors

Table A3. Information security approaches of colleagues in the work group

	Information security approach	Completely disagree	Strongly disagree	Disagree somewhat	Agree somewhat	Strongly agree	Completely agree
1	In this workgroup, we take joint responsibility for ensuring that information security rules are maintained	☐	☐	☐	☐	☐	☐
2	In this workgroup, we remind each other to follow the information security rules	☐	☐	☐	☐	☐	☐
3	In this workgroup, we avoid interfering with how colleagues manage information security (R)	☐	☐	☐	☐	☐	☐
4	In this workgroup, it is accepted that colleagues neglect information security (R)	☐	☐	☐	☐	☐	☐
5	If someone in this workgroup points out a weakness in information security, we try to find a solution	☐	☐	☐	☐	☐	☐
6	In this workgroup group, we learn from our experiences to prevent information security incidents	☐	☐	☐	☐	☐	☐
7	In this workgroup, we take each other's views and suggestions on information security seriously	☐	☐	☐	☐	☐	☐
8	In this workgroup, information security is rarely discussed (R)	☐	☐	☐	☐	☐	☐
9	This workgroup believes that the best way to achieve high information security is through clear information security rules	☐	☐	☐	☐	☐	☐
10	This workgroup finds it difficult to deal with people who are overly concerned about complying with information security rules (R)	☐	☐	☐	☐	☐	☐
11	This workgroup believes that measures to prevent unauthorized access to information are more of a burden than a real benefit (R)	☐	☐	☐	☐	☐	☐
12	In this workgroup, information security rules are mostly for show, because nobody really believes in their benefits (R)	☐	☐	☐	☐	☐	☐
13	There is a consensus in this workgroup that there are real threats to our information technology systems	☐	☐	☐	☐	☐	☐
14	This workgroup believes that it is important to be vigilant against new threats to information	☐	☐	☐	☐	☐	☐
15	This workgroup considers the risk of data breaches to be significantly exaggerated (R)	☐	☐	☐	☐	☐	☐
16	This workgroup considers the risk of threats to information from unexpected sources to be very low (R)	☐	☐	☐	☐	☐	☐

Note(s): Respondents are asked "How do people in your work group approach information security?". Items 1–4 measure Workgroup commitment to information security; Items 5–8 measure Workgroup information security learning; Items 9–12 measure Legitimacy of information security rules in the workgroup; Items 13–16 measure Work group awareness of information security threats. (R) = Reversed item. All items are based on the work of Pousette and Törner (2017)
Source(s): Created by the authors

Appendix 2. Information security leadership behaviors and approaches

Table A4. The information security leadership questionnaire (ISLQ)

	Information security leadership behavior	Never	Almost never	Rarely	Sometimes	Fairly often	Frequently	Always
1	Sets clear information security goals	☐	☐	☐	☐	☐	☐	☐
2	Clarifies how information security goals are to be achieved	☐	☐	☐	☐	☐	☐	☐
3	Expresses clear expectations regarding information security performance	☐	☐	☐	☐	☐	☐	☐
4	Asks for my take on our information security management	☐	☐	☐	☐	☐	☐	☐
5	Encourages me to voice any information security concerns	☐	☐	☐	☐	☐	☐	☐
6	Encourages me to voice suggestions for information security improvements	☐	☐	☐	☐	☐	☐	☐
7	Invites me to participate in improving information security	☐	☐	☐	☐	☐	☐	☐
8	Listens to my ideas and suggestions	☐	☐	☐	☐	☐	☐	☐
9	Uses my suggestions to make decisions that affect me	☐	☐	☐	☐	☐	☐	☐
10	Responds to my ideas, even when they disagree with them	☐	☐	☐	☐	☐	☐	☐
11	Makes decisions based solely on their own ideas (R)	☐	☐	☐	☐	☐	☐	☐
12	Follows up on information security performance	☐	☐	☐	☐	☐	☐	☐
13	I receive positive feedback from my manager when I tell them about information security risks at work	☐	☐	☐	☐	☐	☐	☐
14	I receive positive feedback from my manager when I give suggestions on how to improve information security at work	☐	☐	☐	☐	☐	☐	☐
15	I receive positive feedback from my manager when they see me perform a work task in accordance with information security rules and regulations	☐	☐	☐	☐	☐	☐	☐
16	When I receive positive feedback from my manager, they specifies which behaviors they appreciate	☐	☐	☐	☐	☐	☐	☐

Note(s): Respondents are asked to "describe your perceptions of your immediate manager's information security leadership behaviors. Rate how frequently your manager displays the following behaviors". Items 1–3 measure Information security goal setting (adapted from Sjöberg and Grill, 2024); Items 4–7 measure Information security antecedent listening (adapted from Grill *et al.*, 2023); Items 8–11 measure Information security consequential listening (adapted from Arnold *et al.*, 2000); Items 12–16 measure Information security performance feedback (adapted from Grill *et al.*, 2023 and Sjöberg and Grill, 2024). (R) = Reversed item

Source(s): Created by the authors

Table A5. Information security leadership approaches of managers and supervisors

	Information security leadership approach	Completely disagree	Strongly disagree	Disagree somewhat	Agree somewhat	Strongly agree	Completely agree
1	Management looks the other way when someone neglects information security (R)	☐	☐	☐	☐	☐	☐
2	Management accepts that employees neglect information security when the schedule is tight (R)	☐	☐	☐	☐	☐	☐
3	Management ensures that detected information security weaknesses are corrected immediately	☐	☐	☐	☐	☐	☐
4	In this workplace, management appreciates careful attention to information security, even if it means delaying work	☐	☐	☐	☐	☐	☐
5	Management tries to design information security rules that are meaningful and actually work in practice	☐	☐	☐	☐	☐	☐
6	Management encourages employees to participate in the design of information security rules	☐	☐	☐	☐	☐	☐
7	Management never asks for the input of employees before making decisions related to information security rules (R)	☐	☐	☐	☐	☐	☐
8	Fear of negative consequences from management discourages employees from raising concerns about information security governance (R)	☐	☐	☐	☐	☐	☐
9	Management listens carefully to anyone who has been involved in an incident where information security has been or could be jeopardized	☐	☐	☐	☐	☐	☐
10	Management looks for causes in procedures and systems, not people to blame, when an information security incident occurs	☐	☐	☐	☐	☐	☐
11	Management always puts the blame for information security incidents on employees (R)	☐	☐	☐	☐	☐	☐

Note(s): Respondents are asked "How do you perceive managers and supervisors in this workplace to approach information security?". Items 1–4 measure Management's information security priority; Items 5–8 measure Participative information security management; Items 9–12 measure Non-blaming information security management. (R) = Reversed item. All items are based on the work of Pousette and Törner (2017)
Source(s): Created by the authors