Changing information security behaviour: A field experiment on the effectiveness of security training based on deterrence and vulnerability arguments

Information security policy (ISP) training is a central measure for communicating ISP regulations and imparting ISP procedures to employees. While the general importance of such training is widely acknowledged, few studies have examined how the design of ISP training influences its effectiveness. To fill this research gap, this study sought to understand how personal relevance through deterrence arguments and work relevance through vulnerability arguments can enhance ISP training. We theorize about the process by which ISP training affects employees’ ISP compliance behaviour, arguing for a transfer of training lens to study ISP training effectiveness. The results of our field experiment with triangulated data suggest that the effect of argumentative-enhanced training is twofold: Employees who participated in enhanced training sessions were revealed to have superior learning outcomes. Moreover, they exhibited greater intention to follow ISPs. For actual ISP compliance behaviour, the results only reveal a significant effect for deterrence-based training.

Keywords: information security policy, information security behaviour, transfer of training, field experiment

1 Introduction

A key instrument for achieving information security is information security policy (ISP), which encompasses a set of rules and guidelines related to the processing and use of information within an organization’s boundaries of authority (Baskerville & Siponen, 2002). Enforcing ISP within the company is a key concern of information security managers. For employees, however, following ISP regulations such as password or data encryption policies often impedes work and involves additional effort (Bulgurcu, 2010; D’Arcy & Lowry, forthcoming; Guo, Yuan, Archer, & Connelly, 2011). This can create a conflict between work-related, short-term goals set by the line manager and ISP requirements set by company-wide polices. Moreover, following ISP regulations often
necessitates changing learned work habits, e.g., to comply with clean desk policies (Vance et al., 2012). Therefore, best practices in information security management such as ISO 27002:2013 advocate the implementation of – usually time- and cost-intensive – security education, training, and awareness (SETA) programs (ISO/IEC, 2013). Alongside unidirectional communications and singular awareness campaigns, periodic training sessions are the central means for communicating ISP regulations and imparting knowledge on how to perform the required security procedures efficiently. While research supports the general relevance of these efforts (D’Arcy et al., 2009; Lowry et al., 2015), the gap between prescribed and actual ISP compliance behaviour due to employee negligence still poses a significant threat in securing information (Puhakainen & Siponen, 2010; Guo et al., 2011).

Quantitative studies on the role of SETA programs and training find positive effects on ISP compliance behaviour (D’Arcy & Hovav, 2009). These studies conceptualize SETA programs and training as a unidimensional construct regarding the degree to which organizations have such programs in place and whether employees have received such training (see Table 1). Qualitative studies on changing ISP compliance behaviour delve deeper into the mechanisms of security training. Straub and Welke (1998) stress the need for communication. SETA programs should “convince potential abusers that the company is serious about securing its systems and will not treat intentional breaches of this security lightly” (Straub & Welke, 1998, p.445). Based on learning theories, Puhakainen and Siponen (2010) suggest that “training should utilize contents and methods that activate and motivate the learners to systematic cognitive processing of information they receive during the training” (Puhakainen & Siponen, 2010, p.757). While both qualitative and design-oriented literature emphasize the importance of training design for its efficiency (Straub & Welke, 1998; Puhakainen & Siponen, 2010;
Karjalainen & Siponen, 2011), to the best of our knowledge there is no quantitative empirical research analysing the effectiveness of different training designs on training outcomes and ISP compliance behaviour.

Building upon this gap in existing ISP training literature, this paper aims to further investigate the mechanisms of deterrence and vulnerability arguments in the specific context of ISP training to effectively improve employee ISP compliance behaviour. Accordingly, we posit the following research question: How do personal relevance through deterrence arguments and work relevance through vulnerability arguments influence ISP training effectiveness?

We employ transfer of training literature as the theoretical lens to answer this research question (Baldwin & Ford, 1988; Ford & Weissbein, 1997; Blume et al., 2010). The effect of using vulnerability arguments to communicate work relevance and deterrence arguments to convey personal relevance is twofold: they leverage learning outputs at the training level and also give an important push at the maintenance level when learned procedures are applied. The research model was tested as a field experiment with time-lagged and triangulated behaviour data. Classroom training sessions were designed and conducted as part of a revision of the ISP training procedures of a German energy trading company. Training success in terms of ISP compliance behaviour was measured based on self-reported data directly after the training and secondary data based on two follow-up clean desk controls and one spear phishing campaign.

With this study we contribute to the existing literature in three meaningful ways. First, while current empirical studies primarily adopt a unidimensional perspective on training effectiveness, we compare different training approaches. In doing so, we shed light on the underlying process that accounts for successful training performance and subsequent ISP compliance behaviour. Second, we integrate findings from ISP research on
deterrence and vulnerability. We demonstrate how these mechanisms – which found mixed support in broader ISP compliance studies – can be translated to the specific context of training. Furthermore, we reveal that their effect in ISP training can be twofold. Finally, our research design follows the call for higher external and ecological validity in ISP behaviour research (Lowry et al., 2017; Willison et al., 2018). Our field experiment and data collection is grounded in a real setting with real training sessions and includes measurement of real behaviour with two kinds of secondary data collection.

The remainder is structured as follows. In the next section, we proceed by exploring prior work that has addressed ISP education and training and explain how these inform our study. Drawing on the transfer of training literature, we then develop the research model. The research model integrates deterrence and vulnerability arguments as techniques to increase training output and training generalization in daily work procedures. The subsequent section describes the experimental research approach, including the research setting, training design, and data collection. Afterwards, the statistical analysis is presented. We follow this with a description of the research findings and a discussion of their theoretical and managerial implications, concluding with limitations regarding the interpretations of our results and directions for future research.

2 Literature review

ISPs and SETA programs are two key organizational instruments for achieving information security (Straub & Welke, 1998; D’Arcy et al., 2009). ISPs comprise a set of rules and regulations related to the processing and use of information within the organization’s boundaries of authority (Baskerville & Siponen, 2002). SETA programs
are designed to not only communicate the ISPs but also ensure employee compliance (Peltier, 2005; D’Arcy et al., 2009). They typically involve elements such as security awareness e-mails and newsletters, short briefings, and periodic training courses (Hansche, 2001; Von Solms & Von Solms, 2004).

As part of the SETA program, we understand ISP training as an organizational measure aiming to impart a set of existing policies and teach necessary security skills (Peltier, 2005). Thus, it includes both declarative and procedural knowledge. Declarative knowledge refers to rules and regulations prescribed by the ISPs (i.e., what needs to be done), while procedural knowledge equips employees with the techniques and tools necessary to follow the rules and regulations (i.e., how this can be achieved). For example, the information classification policy specifies a schema that prescribes security requirements for the access, storage, and transmission of sensitive information.

To set this regulation in to practice, the employee must be equipped with tools and knowledge, e.g., when securely sharing confidential files with external partners.

<table>
<thead>
<tr>
<th>Study</th>
<th>Methodology and context</th>
<th>Theories</th>
<th>Conceptualization of SETA</th>
<th>Key findings regarding ISP training</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Albrechtsen &amp; Hovden, 2010)</td>
<td>Longitudinal analysis: Intervention study at a Norwegian public administration agency</td>
<td>Collective reflection</td>
<td>Information security training: Workshop consisting primarily of group discussions vs. no workshop participation</td>
<td>Workshops based on participation, dialogue, and collective reflection in groups increases employees’ reported information security behaviour after the training in comparison to before the training.</td>
</tr>
<tr>
<td>(Chen et al., 2015)</td>
<td>Cross-sectional analysis: Survey on general ISP compliance intention among four companies in the US Midwest</td>
<td>Organizational culture theory</td>
<td>SETA program: Existence of security education regarding computer security responsibilities</td>
<td>Employees’ perceived existence of training sessions improve the security culture and the knowledge of security policies. No significant influence found regarding knowledge about specific policies, rules, and procedures on security culture.</td>
</tr>
<tr>
<td>(D’Arcy &amp; Hovav, 2009)</td>
<td>Cross-sectional analysis: Survey on IS misuse among MBA students at a US</td>
<td>Deterrence theory, deindividuation theory</td>
<td>SETA program: See original scale in (D’Arcy &amp; Hovav, 2007)</td>
<td>SETA programs influence unauthorized access intention. Computer self-efficacy and virtual status moderate this relationship. While the SETA</td>
</tr>
<tr>
<td>Source</td>
<td>Study Design</td>
<td>Methodology</td>
<td>Theoretical Framework</td>
<td>Intervention</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>-------------</td>
<td>-----------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>(D’Arcy &amp; Hovav, 2007; D’Arcy et al., 2009)</td>
<td>Cross-sectional analysis: Professionals from eight US companies. Four scenarios (email usage, user access, software piracy, modification, password sharing)</td>
<td>SETA program: Existence of security education, training, and awareness measures regarding security issues</td>
<td>Deterrence theory</td>
<td>Study (D’Arcy &amp; Hovav, 2007): SETA program has a significant total effect on all five misuse intentions. Study (D’Arcy et al., 2009): SETA program has a significant influence on perceived sanction certainty and sanction severity. Under specific conditions, both mediate the relationship of the SETA program on IS misuse intention.</td>
</tr>
<tr>
<td>(Karjalainen et al., 2013)</td>
<td>Qualitative analysis: Interviews at a global company with locations in Finland, Switzerland, the UAE, and China</td>
<td>Information systems security interventions: Broad perspective on diverse SETA measures</td>
<td>Paradigm of learning</td>
<td>Employees’ preferences regarding the means for learning IS security behaviour vary across national cultures. Learning paradigms should fit with the trainees’ cultures when designing interventions.</td>
</tr>
<tr>
<td>(Lowry et al., 2015)</td>
<td>Cross-sectional analysis: US firms related to financial services. Employee behaviour to reactive computer abuse.</td>
<td>Organizational SETA initiatives: Conduction of training and education</td>
<td>Reactance theory, fairness theory</td>
<td>Organizational SETA initiatives decrease the perception of external control and freedom restrictions and increase explanation adequacy. All three mediate an effect on reactive computer abuse.</td>
</tr>
<tr>
<td>(Puhakainen &amp; Siponen, 2010)</td>
<td>Action research: Finnish software company, email policy training</td>
<td>IS security training program: Fitted ISP training and following IS security communication</td>
<td>Universal constructivist instruction al theory, elaboration likelihood model</td>
<td>The training design that based on learning rather than simple cues and that considers the state of the learner was found to have positive results and was practical to deploy. Training should be accompanied by continuous IS security communication.</td>
</tr>
<tr>
<td>(Straub &amp; Welke, 1998)</td>
<td>Action research: Two companies in information technology services in the US</td>
<td>Education/trainin g in security awareness: Broad perspective on training as part of SETA initiative</td>
<td>Deterrence theory</td>
<td>The results suggest that awareness training should emphasize sanction certainty and severity to motivate compliance behaviour. Training materials should communicate not only higher-level concepts, such as the security action cycle (i.e., deterrence feedback mechanism), but also detailed</td>
</tr>
</tbody>
</table>
Empirical studies on the intersection of SETA programs, ISP training, and ISP compliance behaviour are depicted in Table 1. Overall, the findings support the important role that SETA programs and ISP training play in determining employee ISP compliance behaviour. In all cross-sectional, quantitative empirical studies, the variable that captures the SETA program is conceptualized as the individual’s perception of SETA measures within the organization (D’Arcy & Hovav, 2007; D’Arcy et al., 2009; D’Arcy & Hovav, 2009; Putri & Hovav, 2014; Lowry et al., 2015; Talib & Dhillon, 2015; Chen et al., 2015; Hovav & Putri, 2016). Moreover, two studies find a significant effect of SETA programs and knowledge about security policies (D’Arcy & Hovav, 2007; Chen et al., 2015). This indicates the importance of SETA for policy communication. In regard to individuals’ ISP compliance, the SETA variable is either set as a direct antecedent of compliance behaviour (D’Arcy & Hovav, 2007; D’Arcy & Hovav, 2009; Albrechtsen & Hovden, 2010) or set in a nomological network with mediating factors based on deterrence, motivation, or other psychological or organizational theories (D’Arcy et al., 2009; D’Arcy & Hovav, 2009; Putri & Hovav, 2014; Lowry et al., 2015; Talib & Dhillon, 2015; Chen et al., 2015; Hovav & Putri, 2016). One study collected longitudinal data and analyses of the effect of group-based training on compliance behaviour (Albrechtsen & Hovden, 2010). The researchers designed a training session for an intervention group based on participation, dialogue, and collective reflection. A paired analysis of reported ISP compliance behaviour before and after the training course reveals a significant increase for three out of four security
behaviours. For a control group that received no training, only one out of the four behaviours improved significantly. The basic assumption in all quantitative studies is that the SETA programs are unidimensional in nature. The training itself or the perception of the existence of SETA programs directly affects the mediators or the behaviour variables. If moderators are introduced, they refer to individual characteristics that interact with the influence of the SETA program (D’Arcy et al., 2009; D’Arcy & Hovav, 2009).

The qualitative studies in our sample extend this conceptualization of SETA programs. In an action research study, Straub and Welke (1998) find evidence that training effectiveness depends on deterrence measures as part of the training process. A major goal is to “convince potential abusers that the company is serious about securing its systems” (Straub & Welke, 1998, p.445). Puhakainen and Siponen’s (2010) action research study dismantles the learning process of the security training. They propose an information security training course based on a learning theory and a behavioural change theory. The results suggest that a learner’s systematic cognitive processing of information should be activated within an information security training session. Furthermore, learning tasks should be of personal relevance and the training should be oriented toward the learner’s knowledge. The results of Karjalainen et al.’s (2013) qualitative analysis suggest that the cultural dimension should be considered in training design, as different cultures prefer different learning and communication methods. The overarching findings of the qualitative studies fit with the design recommendations of non-empirical research. For example, Karjalainen and Siponen (2011) develop a meta theory on information security training and define pedagogical requirements. Siponen’s (2000) structured approach to SETA programs is based on persuading techniques such as morals and ethics, well-being, a feeling of security, rationality, logic, and emotions. It
also emphasizes the importance of normative approaches and motivational and
behavioural theories in the context of SETA programs.

The existing empirical literature in the field of SETA programs and ISP training informs
this research in two areas. First, there is a gap between training conceptualization and
quantitative empirical evidence. While the two action research studies suggest
considering the learning process, all quantitative studies conceptualized training as
unidimensional, i.e., training has a generally positive effect on compliance behaviour.
None of the quantitative studies consider the effectiveness of different training
approaches. Therefore, further conceptualization and quantitative empirical evidence is
needed to strengthen the learning perspective and better understand the mechanisms of
ISP training. Second, all quantitative empirical findings regarding the link between
SETA programs and compliance behaviour are based purely on self-reported data. With
the exception of one longitudinal study, all quantitative studies based their results on
cross-sectional and correlational analyses. An experimental design with time-lagged and
secondary data would increase the rigorousness of the findings.

3 Research model

In this study, we aim to understand whether and how the inclusion of personal relevance
and work relevance through deterrence arguments and vulnerability arguments can
enhance SETA programs. Our research model is guided by the transfer of training
literature and the respective dominant nomological network of the transfer process
(Baldwin & Ford, 1988; Ford & Weissbein, 1997). The transfer process comprises three
stages: training inputs, training outputs, and conditions of transfer. Starting with the last
stage, the conditions of transfer describe the generalization of learned training
procedures to the work context and the maintenance of that behaviour over time. The
training outputs refer to the new knowledge gained during the training and the retention
of that knowledge after the training is completed. The training inputs include the
training design and the characteristics of the trainee and the work environment. As a
first premise, the transfer process argues that training material must be learned (i.e.,
training output) before it can be applied to the job (i.e., conditions of transfer). The
second premise is that the trainee’s learning success (i.e., training output) is dependent
not only on the training session’s content but also on individual preconditions for
learning and reinforcing environmental work characteristics (i.e., training inputs). The
third premise of the transfer process is that training inputs also have a direct influence
on conditions of transfer. Procedures and skills learned during training are more likely
to be applied at work if individual and environmental characteristics reinforce the
behaviour. The transfer of training literature contends that training coupled to the
organizational transfer climate, e.g., in terms of process and reward systems, allows for
superior transfers (Blume et al., 2010).

We translate the transfer process to training concerning declarative and procedural ISP
knowledge and ISP compliance behaviour. In line with the transfer process, we posit
that a transfer gap between trained and actual compliance behaviour can arise. If the
work environment does not reinforce desired behaviour, well-learned skills may not be
maintained on the job. To be more specific, we interpret deterrence arguments and
vulnerability arguments as methods of communicating to trainees the personal relevance
and work relevance, respectively, of ISP compliance behaviour. The effect of the
personal and job relevance is twofold: First, if the training emphasizes relevance for the
employee, s/he will be more motivated to undertake the cognitive processing of
declarative and processual knowledge. Second, an awareness of its relevance also
motivates compliance behaviour at the generalization and maintenance stage. Drawing
on these fundamental transfer of training mechanisms, we contend that deterrence
arguments (i.e., personal relevance) and vulnerability arguments (i.e., work relevance) can leverage the effectiveness of ISP training. The research model is depicted in Figure 1.

Embedding our research model within the transfer of training literature is suitable for two main reasons. First, the transfer of training literature provides a solid framework that is both theoretically well-grounded and empirically established. It has been applied in a variety of organizational training courses, including leadership training, technical training, and computer training (Blume et al., 2010). Unlike other measures of information security management systems, such as policy design or other SETA measures (e.g., one-way email communication), ISP training imparts knowledge on both regulations and procedural requirements. ISP training can therefore be seen as a form of organizational training that imparts security skills. Second, transfer of training literature allows two streams to be integrated from the more general research on information security behaviour to the specific context of ISP training. More specifically, the transfer of training process sheds light on the mechanisms of deterrence through sanctions and protection motivation through vulnerability, revealing how they distinctively leverage the acquisition of knowledge, the expected compliance behaviour, and the actual compliance behaviour.
3.1 The influence of personal relevance through deterrence arguments

A common measure for ensuring that employees adhere to ISP regulations is the implementation of deterrence. Organizations implement disciplinary sanctions including disciplinary warnings, fines, demotions, and dismissals (Herath & Rao, 2009a; Johnston et al., 2015). Drawing on deterrence theory from criminology research, it is argued that the more severe the sanctions are and the more likely they are to apply, the more likely employees are to follow the regulations (Peace et al., 2003; D’Arcy & Herath, 2011). In line with this mechanism, it is recommended that policies be designed to implement deterring sanctions and measures for detecting deviant behaviour. We translate this deterrence perspective to training design and argue that deterrence arguments can be a powerful tool in ISP training.

The effect of deterrence-based messages on attitude changes and adaptive behaviours finds wide support across diverse fields, such as earthquake preparation, health behaviour, and criminal behaviour (Gleicher, 1990; Peters et al., 2013). In this paper,
deterrence arguments refer to deliberately placed messages in the communication process that arouse fears related to the threat of individual sanctions. Personal relevance is elicited by messages stressing that formal or informal sanctions are to be expected if employees deviate from policy regulations. The messages include both the severity of the sanctions and the certainty with which they will apply.

In line with the transfer of training literature (Ford & Weissbein, 1997), the effect of deterrence arguments in information security training is twofold. The arousal through deterrence arguments increases an employee’s motivation to participate in the training procedures instead of ignoring them. Participants are thus more aware of the trained security knowledge. Moreover, trained procedures are also more likely to be applied. This is in line with the findings from Puhakainen and Siponen’s (2010) action research study on ISP training design. Their results suggest that training should implement methods that activate and motivate the trainee to increase systematic cognitive processing of training content. When trained procedures need to be applied in a real work setting, fear arousals are connected to the procedural knowledge. Employees then take this into account when deciding for or against a deviant behaviour, and are therefore more likely to follow prescribed procedures. Accordingly, we propose the following hypotheses:

Hypothesis 1a (H1a): Deterrence arguments increase the effect of ISP training on ISP knowledge.

Hypothesis 1b (H1b): Deterrence arguments increase the effect of ISP training on intended ISP compliance behaviour.

Hypothesis 1c (H1c): Deterrence arguments increase the effect of ISP training on actual ISP compliance behaviour.
3.2 *The influence of work relevance through vulnerability arguments*

A threat vector that arises from insecure information security behaviour might lead not only to personal sanctions for the employee, but the threat vector itself can also affect the employee’s work, her/his team, or the entire organization. Vulnerabilities can involve data, information, and information systems in terms of confidentiality, integrity, and availability (Johnston *et al.*, 2015). Based on protection motivation theory, some studies have related security threats and probabilities of exposure to information security behaviour (Herath & Rao, 2009b; Putri & Hovav, 2014; Menard *et al.*, 2017).

In the following, we adapt the idea of work-related vulnerability to the framework of security training.

Fear appeal messages can build upon the work relevance of security threats as part of the security training, relaying vulnerability arguments emphasizing that a security threat can impose significant damages or disturbances. The daily work, the team, or the entire company can be affected. If one fails to follow the security regulations, such threats are likely to cause severe damage. The nature of deterrence arguments is different from that of vulnerability arguments: while the first refers to consequences imposed on the trainee by the organization, the latter sees the trainee as part of the organization exposed to external threats (Johnston *et al.*, 2015). According to the transfer of training literature, such messages during the training sessions motivate trainees to learn the procedures, align their expected behaviour with the regulations, and reinforce desired security behaviour in working life. We therefore posit the following hypotheses:

Hypothesis 2a (H2a): Vulnerability arguments increase the effect of ISP training on ISP knowledge.

Hypothesis 2b (H2b): Vulnerability arguments increase the effect of ISP training on intended ISP compliance behaviour.
Hypothesis 2c (H2c): Vulnerability arguments increase the effect of ISP training on actual ISP compliance behaviour.

### 3.3 The influence of employee characteristics and ISP knowledge

With our study we primarily aim to identify the true effect of deterrence- and vulnerability-enhanced ISP training on ISP knowledge and compliance behaviour. However, to control for other effects, we introduce employee characteristics and ISP knowledge into the research model as further explanatory variables. First, we complete the transfer of training perspective with a set of controls for individual trainee characteristics. These include gender, age, education, and job tenure. Such a set of individual characteristics is typical in IS security literature on information security behaviour (Straub & Welke, 1998; D’Arcy et al., 2009; Bulgurcu, 2010; Chen et al., 2013). We thus use these variables as covariates for the influence of ISP training on ISP knowledge and ISP behaviour.

Second, we include the effect of ISP knowledge on ISP behaviour in our model. In line with the transfer of training literature, we argue that employees are more likely to follow ISP regulations if they are properly equipped with declarative and procedural knowledge (Baldwin & Ford, 1988). Awareness of the knowledge is necessary for the willingness to comply with the ISP. Related ISP awareness studies have already found evidence that compliant behaviour is related to the knowledge and understanding of rules and regulations prescribed by the ISP (Bulgurcu, 2010; Rocha Flores et al., 2015). We therefore introduce ISP knowledge into the model as a covariate to ISP behaviour.

### 4 Method

This experimental field study follows a between-subjects design with three treatments, which were conducted as part of a revised ISP compliance training of an energy trading
company in Germany (Appendix A depicts a more detailed description of the study context and implementation). Each treatment was conceived as a training session that imparts declarative and procedural ISP knowledge. While two training sessions were enhanced with deterrence arguments and vulnerability arguments, the third served as the baseline control group with no additional arguments (Appendix B includes a more detailed description of the training content). In the following, we explain the ex-ante power analyses and measurement of research variables.

4.1 Ex-ante power analysis

In experimental research designs, a power analysis is used to determine the sample size sufficient to achieve an adequate power. Based on comparable transfer of training literature (Tracey et al., 1995; Facteau et al., 1995), effect sizes for the training sessions were estimated to be medium to large ($f = .325$). The power analyses assumed an $\alpha$-error probability of .10 and a statistical power of .80. A power analysis in G*Power revealed that the lower threshold for the sample size of a one-way ANOVA with three groups is 66 participants (Faul et al., 2007; Faul et al., 2009). When the study design was established, the sample size was estimated to be around 90 qualified questionnaires from trained employees and 80 valid answers for actual behaviour. Accordingly, we opted for an experimental between-subjects design with three groups. This was preferable to other designs, such as a full factorial design, due to its lower group-size requirements. The treatment of each group differed in terms of deterrence arguments and vulnerability arguments; a baseline group served as the control.

4.2 Measurement of variables

Research variables were measured based on a questionnaire, a fake spear phishing campaign, and two clean desk checks. The questionnaire served as an instrument to measure individual characteristics, ISP knowledge, and intended ISP compliance. After
a discussion of the merits and disadvantages of hypothetical and behavioural measurement, intended ISP compliance behaviour was measured as situational and generic ISP compliance intention. The spear phishing campaign and the clean desk checks served as objective measures for actual ISP compliance behaviour. A detailed description of the instruments can be found in Appendix C.

The research design, hypothetical scenarios, and scales were evaluated by a total of nine experts: four internal information security experts, one internal expert on data protection, one external information security consultant, and three experts in IS research. As a result of this pilot testing, the wording of some items and scenarios in the training materials were adjusted in several correction loops. Ultimately, the training material was deemed effective, the scenarios were determined to be as realistic and logical possible, and the scales were regarded as valid in terms of content validity.

5 Data analysis and results

We used IBM SPSS Statistics 25 for a descriptive analysis of the questionnaire data, an exploratory factor analysis to check for psychometrical properties of the scales, and the analysis of the actual ISP compliance behaviour data. IBM SPSS Amos 25 was used to conduct covariance-based structural equation modelling and to analyse the treatment effects on the latent behavioural measures.

5.1 Descriptive statistics and manipulation checks

The demographic characteristics of the sample that received the training (N = 88) exhibit a typical distribution for the company. The average age in the sample is 39.9 years with an average job tenure of 12.8 years. The vast majority of the sample (84%) earned a university degree, and around 56% of the sample is male. The profile of the sample suggests that the participants are educated and experienced.
Manipulation checks were conducted to test the effectiveness of the treatments. We used two items to check for the manipulation of the deterrence arguments. For formal sanctions, an item was adapted from Siponen and Vance (2010) that asks, “What is the chance you would receive disciplinary consequences if you violated the company information security policy?” To account for informal sanctions, we adapted an item from Johnston et al. (2015) and asked, “What is the chance of losing the respect and approval of my colleagues (e.g., Clean Desk Policy)?” A one-way multivariate analysis of variance (MANOVA) was conducted, revealing the groups to be significantly different ($F_{2,88} = 6.167, p < .01$). We derived one item from Ifinedo (2012) to check for the manipulation of the vulnerability arguments. The item states, “I could fall victim to a malicious attack if I fail to comply with my organization’s IS policy.” The second item refers to the response efficiency in regard to vulnerability: “Enabling the security measures on my work computer is an effective way to protect me from hacker attacks.” Again, we ran a one-way MANOVA, which revealed significant differences ($F_{2,88} = 2.811, p < .05$). The results of the manipulations checks provide strong evidence that the trainees correctly interpreted the treatments in terms of deterrence and vulnerability arguments.

5.2 Results for ISP knowledge and intended ISP compliance behaviour

Because there were two latent variables, we decided to apply a structural equation approach with a maximum likelihood estimator for the analysis. Table 2 presents the results of the estimation. The model appears to have good measurement properties (Hu & Bentler, 1999). The chi-square test becomes insignificant ($p > .10$), the CFI is above the threshold of .95, and the RMSEA is below the threshold of .07. Hence, we conclude that the estimated model has good measurement properties.
The results provide full support for hypotheses H1a and H1b. The effect of training enhanced with deterrence arguments on ISP knowledge and on the two sub-dimensions of ISP compliance intention become significant in this experiment. For training with vulnerability arguments, we find a significant effect on ISP knowledge, offering support for hypothesis H2a. The results are mixed for hypothesis H2b and the effect on ISP compliance intention. While we find a significant effect for vulnerability arguments on general ISP compliance intention, the effect on situational ISP compliance intention remains insignificant.

We find three significant effects for the non-experimentally manipulated variables. First, our data suggests that education influences ISP knowledge. Second, we find a significant negative correlation between job tenure and situational ISP compliance intention. Third, we find partial support for the role of knowledge. The data reveals a significant effect on general ISP compliance. The effect on situational ISP compliance intention remains insignificant.
### Table 2. Results for ISP knowledge and intended ISP compliance behaviour.

| | ISP knowledge | | | Intended ISP compliance behaviour | | |
|---|---|---|---|---|---|
| | b (SE) | p-value | | b (SE) | p-value | | b (SE) | p-value |
| **Experimental dummy variables**<sup>1</sup> | | | | | | | | |
| Training with | | | | | | | | |
| … deterrence arguments | .220 (.118) | .031* | .228 (.126) | .035* | .191 (.115) | .049* |
| … vulnerability arguments | .189 (.118) | .059* | .240 (.125) | .028* | .104 (.114) | .181 |
| **Covariate variables** | | | | | | | | |
| ISP knowledge | | | | | .111 (.113) | .161 | .421 (.106) | .001** |
| Gender | -.125 (.101) | .109 | .033 (.109) | .381 | .094 (.098) | .169 |
| Age | -.097 (.177) | .292 | .227 (.185) | .110 | -.066 (.169) | .349 |
| Job tenure | .107 (.176) | .272 | .254 (.186) | .085* | .100 (.167) | .277 |
| Education | .201 (.101) | .024* | .015 (.112) | .446 | .018 (.101) | .429 |
| **Squared multiple correlations** | | | | R<sup>2</sup> = .102 | R<sup>2</sup> = .102 | R<sup>2</sup> = .240 |
| **Model fit parameters** | chi-square = 43.681; df = 39; p = .279; CFI = .988; RMSEA = .037 |

Results based on structural equation modelling with maximum likelihood estimation. <sup>1</sup> Coded as dummy variables with the baseline training as reference group; * p < .10; ** p < .01; p-value = probability of error that is based on a one-tailed t-test; N (total) = 88; n (training with deterrence arguments) = 31; n (training with vulnerability arguments) = 28; n (control group) = 29; b = standardized path coefficient; SE = standard error of the estimator; df = degrees of freedom; CFI = Comparative Fit Index; RMSEA = Root Mean Square Error of Approximation.

### 5.3 Results for actual ISP compliance behaviour

As noted earlier, actual behaviour was measured in terms of email policy behaviour and clean desk policy behaviour. Due to privacy concerns and to assure anonymity, data collection did not relate the individual questionnaire answers to the actual behaviour. Instead, information was collected at the training group level. As the dependent variables are dichotomous, a two-way chi-square test was conducted to determine whether the group distributions differ in terms of non-compliant behaviour. For email policy behaviour, this implies clicking on a link in the phishing email. For the clean desk policy, non-compliant behaviour was determined to entail not locking the laptop in the docking station or leaving confidential information openly accessible. The results of the analysis are depicted in Table 3.
Table 3. Results for actual ISP compliance behaviour.

<table>
<thead>
<tr>
<th>Table 3. Results for actual ISP compliance behaviour.</th>
<th>First measurement t₃,₄</th>
<th>Second measurement t₅</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>NC (%)</td>
</tr>
<tr>
<td>Spear phishing campaign: clicked on phishing link in email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Training with deterrence arguments</td>
<td>31</td>
<td>19.4</td>
</tr>
<tr>
<td>B. Training with vulnerability arguments</td>
<td>25</td>
<td>28.0</td>
</tr>
<tr>
<td>C. Baseline training (control group)</td>
<td>25</td>
<td>40.0</td>
</tr>
<tr>
<td>No training¹</td>
<td>34</td>
<td>38.2</td>
</tr>
<tr>
<td>Clean desk policy: notebook locked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Training with deterrence arguments</td>
<td>19</td>
<td>36.8</td>
</tr>
<tr>
<td>B. Training with vulnerability arguments</td>
<td>15</td>
<td>33.3</td>
</tr>
<tr>
<td>C. Baseline training (control group)</td>
<td>13</td>
<td>30.8</td>
</tr>
<tr>
<td>No training¹</td>
<td>20</td>
<td>35.0</td>
</tr>
<tr>
<td>Clean desk policy: confidential information accessible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Training with deterrence arguments</td>
<td>24</td>
<td>33.3</td>
</tr>
<tr>
<td>B. Training with vulnerability arguments</td>
<td>18</td>
<td>16.7</td>
</tr>
<tr>
<td>C. Baseline training (control group)</td>
<td>18</td>
<td>16.7</td>
</tr>
<tr>
<td>No training¹</td>
<td>22</td>
<td>22.7</td>
</tr>
</tbody>
</table>

Note: ¹ The no training-group comprised of randomly selected employees from the population of employees with no need for a training in the current ISP training round, i.e., in most cases they received a training in the past year. Thus, training group C serves as the baseline for further statistical comparisons; n = sample size; NC = non-compliance with ISP; * p < .10; ** p < .01; p-value = probability value based on a two-way chi-square test between the baseline training and the enhanced training. t₃,₄ = refers to timeframe 4 for the phishing campaign and timeframe 3 for the first clean desk control; t₅ = refers to timeframe 5 for the second clean desk control.

The results for the email-based spear phishing campaign are mixed. The sample for the analysis consists of 81 participants, 5 of which were excluded due to out of office notifications. The results show that 19.4% of the employees in the deterrence-based training group fell for the trap of the spear phishing email, compared to 28% for the vulnerability-based training group and 40% of the control group. A comparison between the deterrence-based training group and the control group show a significant difference (p < .10). This offers support for the effect of deterrence arguments on actual behaviour for the phishing campaign (H1c). We find no significant difference for the effect of vulnerability arguments (H2c).

In regard to clean desk policy compliance, the sample size for the accessible confidential information is 80 observations for both time points of measurement. The drop in participants is due to some offices being inaccessible for the checks. The sample size for locked notebooks is 47 and 46 for time points 1 and 2, respectively. Alongside
office accessibility, this reduced number can also be explained by the absence of some notebooks from the office at the time of control. No clear pattern is discernible in regard to the mean values between both clean desk categories. The results of the pairwise distribution tests support this observation for all comparisons ($p > 10$). Thus, we find no support for hypotheses H1c and H2c for clean desk policy compliance behaviour.

For an explorative outlook for general training effectiveness, we also collected actual ISP compliance data from a sample of employees who did not take part in the current round of ISP trainings. In contrast to the three training groups, they were drawn from the population of employees who needed no training in the current round of ISP trainings. This means that most of them participated in a training session one year ago. A comparison with the baseline training shows no significant difference (see results for “no training” in Table 3).

6 Discussion

This study sought to understand how personal relevance through deterrence arguments and work relevance through vulnerability arguments can enhance ISP training to improve their effectiveness. In line with the transfer of training literature, we set them in the nomological net of the transfer process. We argued that training with enhanced elements in terms of deterrence and vulnerability arguments has improved learning outcomes concerning ISP knowledge. Moreover, we posited that enhanced training leads to a higher level of employee ISP compliance behaviour. To test the research model, we conducted a field experiment in a German energy trading company. Different training sessions were designed and conducted as part of a project revising the implementation of their information security management. Overall, the results confirm partial or full support for five of the six hypotheses, indicating substantial backing of the
theoretical model and the applicability of the transfer of learning perspective. The results are summarized in Table 4.

Table 4. Summary of study results.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Evidence</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Experimental effects of deterrence arguments</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H1a. Training with deterrence arguments → ISP knowledge</td>
<td>Trainees in this setting reported a significantly greater degree of ISP knowledge.</td>
<td>Yes</td>
</tr>
<tr>
<td>H1b. Training with deterrence arguments → intended ISP behaviour</td>
<td>Both situational and general ISP compliance intention was significantly higher for participants of this training session.</td>
<td>Yes</td>
</tr>
<tr>
<td>H1c. Training with deterrence arguments → actual ISP behaviour</td>
<td>Trainees were less prone to the spear phishing attack. In regard to clean desk behaviour, no significant effects can be observed.</td>
<td>Partial</td>
</tr>
<tr>
<td><strong>Experimental effects of vulnerability arguments</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2a. Training with vulnerability arguments → ISP knowledge</td>
<td>Trainees in this setting reported a significantly higher degree of ISP knowledge.</td>
<td>Yes</td>
</tr>
<tr>
<td>H2b. Training with vulnerability arguments → intended ISP behaviour</td>
<td>Only situational but not general ISP compliance intention was significantly higher for participants of this training group.</td>
<td>Partial</td>
</tr>
<tr>
<td>H2c. Training with vulnerability arguments → actual ISP behaviour</td>
<td>A significant effect cannot be found for the phishing campaign nor for clean desk behaviour.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Correlational effects of transfer of training controls</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP knowledge → intended ISP behaviour</td>
<td>ISP knowledge significantly increases general ISP compliance intention. The effect on situational ISP knowledge remains insignificant.</td>
<td>Partial</td>
</tr>
<tr>
<td>Employee characteristics → intended ISP behaviour</td>
<td>The level of education significantly increases ISP knowledge. Job tenure significantly contributes to the explanation of differences in situational ISP compliance.</td>
<td>Partial</td>
</tr>
</tbody>
</table>

Note: * In comparison to the training without a specific additional argument

The first noteworthy finding refers to the substantial overarching support of the effect of deterrence arguments on training effectiveness. We find that deterrence arguments can work at all three stages, i.e., knowledge acquisition, intended ISP behaviour, and actual behaviour. The estimated effect of vulnerability arguments is smaller for general compliance intention and the spear phishing campaign. From a substantive perspective, this suggests that deterrence arguments were more effective in our sample training groups than the vulnerability arguments were. In light of the discussion around the merits of deterrence theory in ISP compliance studies (Willison et al., 2018), our results support the deterrence perspective for ISP training. Moreover, our results contribute to the findings of Herath and Rao (2009b) and Johnston et al. (2015) regarding the distinctive effects of vulnerability and deterrence for ISP compliance behaviour.
Interestingly, we find a gap between intended behaviour and actual compliance in our data. While our data reveals that enhanced training has substantial predictive power for intended behaviour measures, its influence on actual behaviour remains mixed. There are several potential interpretations for this intention–behaviour gap. One explanation can be found in the length of time between the measurement of intended and actual behaviour: Though the deterrence and vulnerability arguments led to temporary changes of beliefs regarding ISP behaviour, the lasting effects are diminishing. Another explanation could be an individual’s low levels of volition, such as regards self-regulation, conflicting goals, or habitual behaviour. These effects are typical in intervention research and can also be found in fields such as health behaviour (Orbell & Sheeran, 1998) or consumer psychology (Carrington et al., 2010). In line with the transfer of training literature (Ford & Weissbein, 1997), continuous reinforcement in the work environment can help bridge this gap. In the same vein, Puhakainen and Siponen (2010) recommend an ongoing ISP communication procedure after initial ISP training.

Delving deeper in to the results of actual ISP behaviour, we find an interesting difference between the spear phishing campaign and the clean desk behaviour. The spear phishing campaign seems to have a pattern regarding the influence of the enhanced training that is similar to the case of intended ISP compliance behaviour. However, for clean desk behaviour, the estimated effects of the baseline and vulnerability groups do not differ and the comparison with the deterrence group is even negative. It appears that the enhanced training had no effect on clean desk behaviour. One explanation for this can be found in the type of behaviour. The behaviour relevant to the clean desk policy can be regarded as rather habitual. In contrast to the conscious evaluation of an email that was necessary for the spear phishing scenario, keeping your documents in order and locking your computer are long-term learned and unconscious
daily routines. While our results support the argument that enhanced training can change knowledge and intended behaviour, changing habits in terms of actual behaviour requires more effort than conducting a single training session. This also fits with habit research on the gap between intention and behaviour (Limayem et al., 2007) and complements research on habit formation and past behaviour in information security research (Vance et al., 2012; Chatterjee et al., 2015; Anderson et al., 2016; Vance et al., 2018).

We also find interesting effects of ISP knowledge. As hypothesized, there was a substantial significant effect on general ISP compliance intention, supporting the role of knowledge acquisition as a necessary precondition in the transfer process. However, the absolute effect on situational ISP compliance intention is smaller and insignificant. At first sight, this seems surprising, as we provided dedicated procedural knowledge for specific security behaviours. One explanation for this is that knowledge about the ISP and the procedures generally leads to greater acceptance of the ISP at the overarching level. Employees might be not fully aware of efforts related to the secure behaviour. However, when it comes to specific behaviours in which employees are directly confronted with conflicting goals and work impediments, these factors become more important than ISP knowledge.

Finally, we also exploratively looked at the general role of training effectiveness. When comparing the baseline training that only addresses “what” and “how” with people who received no dedicated training in this round, we find no evidence for a change of actual ISP compliance behaviour. We interpret this results as a further indication for the importance of addressing “why”. Moreover, this result suggests that training can only be one building block for a sustainable change of employees’ ISP behaviour.
6.1 **Theoretical contributions**

Our results provide three major theoretical implications for IS research. First, our research theorized about the underlying process by which ISP training affects employee ISP compliance behaviour, arguing for a transfer of training lens to study ISP training effectiveness. Our work extends the unidimensional perspective of SETA, i.e., its pure existence or perception of existence. It is the first to find empirical support for the effect of security training enhanced with either deterrence or vulnerability arguments. Second, this paper contributes to the literature on deterrence and protection motivation that aims to explain ISP compliance behaviour. We conceptualized the deterrence and vulnerability perspective to the training context and were able to demonstrate that the effect of training can be twofold: it enhances training output as well as generalization to the working context. Moreover, a post hoc comparative assessment suggests that deterrence and vulnerability work differently in our setting, depending on the type of security behaviour. This assessment contributes to the discussion on rewards and punishments in ISP studies (Bulgurcu, 2010; Chen *et al.*, 2013). For comparative analyses, context dependency might provide a fruitful avenue. Third, this paper contributes to the methodological discussion in ISP compliance behaviour research. In the same vein as the results for the field of SETA studies (see Table 1), senior scholars in the field of ISP behaviour criticize that ISP studies often rely on intentional or hypothetical behaviour measures with cross-sectional, self-reported data (Lowry *et al.*, 2017; Willison *et al.*, 2018). We are among the first to find a time-lagged effect of deterrence theory for ISP policy behaviour in a field experiment. In doing so, we contribute to the discussion about the merits of deterrence theory in ISP studies and provide compelling evidence that deterrence mechanisms can work in specific organizational settings. Moreover, our training was revealed to have a meaningful effect
on self-reported and expected behaviour in terms of situational ISO compliance. The training effect on actual, time-lagged behavioural change, however, only found limited support. Our results thus strengthen the call for more compelling evidence based on more rigorous data collection to underline the validity and generalizability of research findings for both research and practice (Lowry et al., 2017).

This research also provides important contributions to practice. First, our results empirically underline the ISO 27002:2013 implementation recommendation for SETA programs (ISO/IEC, 2013). Information security managers are recommended to design their training to address the questions of not only what and how but also why. More specifically, our design for a protection artefact (Lowry et al., 2017) recommends that both the personal and work relevance of ISP behaviour should be emphasized as part of the training process. Compared to other procedural and technical measures, this can be a cost-efficient improvement. Second, our results highlight the importance of knowledge acquisition for ISP compliance behaviour. ISPs are not an end unto themselves. To gain value from ISPs, regulations must be communicated appropriately and the necessary skills need to be trained. As demonstrated within this study, compelling relevance arguments can even increase the effect. Third, our data suggests that single security training sessions are no silver bullet. Our results offer substantial evidence that enhanced ISP training shows good support for changing intended behaviour. However, changing actual compliance behaviour, especially habitual security behaviour, seems to be more challenging. We therefore emphasize the importance of not designing ISP training in isolation. Instead, managers should favour a holistic approach of SETA programs that sees ISP training as tool for nudging security behaviour in the right direction but at the same time addresses changes to the work environment. Finally, while our results guide organizations on how to reduce the security risks arising from
human errors, the findings also reveal that humans are still a weak link in the information security chain. Though the spear phishing campaign impressively demonstrated the important role of enhanced ISP training, even a few employees being tricked into clicking a malicious link could be enough to compromise internal networks. Information security managers should be aware of this important residual risk and have appropriate counter measures in place.

6.2 Limitations and future research

Having presented our results, we must discuss some limitations stemming from the choice to conduct a field experiment in a single company and following limiting factors in research design. First of all, care must be taken when generalizing these results to other contexts. The study was conducted in a single company of the energy trading industry with a sample of mainly German employees with an above average level of education and a high importance of information security. However, research suggests that cultural factors affect ISP compliance behaviour (Hovav & D’Arcy, 2012; Mou et al., 2017) and ISP training success (Karjalainen et al., 2013). Moreover, our results are based on the analysis of 88 participants yielding behavioural responses to three hypothetical scenarios, and one general compliance measure. Of these, only 46–81 participants were included for measuring the two actual behaviours. The weaker statistical power of a small sample size can be seen as another limitation – in particular, the possibility of type II errors. Some influences are meaningful in terms of effect size but analysis finds no significant different effect from zero. Finally, the experimental manipulation was conducted in training groups, as this is a typical approach for classroom training. While we tried to keep group-level variables constant across the groups, e.g., in term of time, training rooms, and training facilities, some unobserved group-level variables might have biased the results. To allow for wider generalizability
of this study’s findings, research is necessary, e.g. a laboratory experimental research
design with hypothetical scenarios and a greater number of observations.
This study also creates several opportunities for further research. An interesting avenue
would be to delve deeper into the differences among the effects of the argumentative
enhancements. This study focused on establishing some basic mechanisms of the
transfer process in the ISP training context. Elaborating upon which training
enhancements or even which combination of argumentative enhancements is superior
from a substantive perspective could provide important answers for both researchers
and practitioners for effective training design. This can also be translated to the cross-
cultural context. Karjalainen et al. (2013) find support that ISP interventions based on
deterrence mechanisms might work for some countries while having an inverse effect in
others. Providing ISP training design artefacts that account for differences among
cultures is particularly interesting for cross-national organizations. Finally, next to the
focus on work and personal relevance as components of training design and work
environment, the transfer of training perspective offers interesting directions to further
integrate existing ISP compliance behaviour research into the training context. For
example, further research could build upon ISP research on personality (Warkentin et
al., 2012; Johnston et al., 2016) and integrate it into the duality of the transfer of
training process. Moreover, examining the role of the work environment in terms of
organizational information security culture (Chen et al., 2015; Guhr et al., 2018)
through the lens of the transfer process can shed light on the question of when trained
ISP procedures are generalized and maintained in daily work routines.
References


Information Systems 29(3), 157–188.


HOVAV A and PUTRI FF (2016) This is my device! Why should I follow your rules?


PETERS GJY, RUITER RAC and KOK G (2013) Threatening communication: A


**Appendix**

**Appendix A. Study context and implementation**

The host company is one of Germany’s leading energy trading companies. The firm’s employees primarily work in information-intensive processes across countries in Europe. Due to a high reliance on process automation and information systems, information security has long played a central role in the company’s management. The
recent announcement of a new German regulation regarding critical infrastructure further increased the importance of information security, and the firm revised its information security management accordingly. As one key measure, the management decided to update their information security training approach. Information security training sessions are part of the information security management system’s awareness measures. Employees are trained regularly, starting at the beginning of their appointment and then approximately every two years. As depicted in the following figure, the research design follows three steps.

In the first step, we prepared the training material and identified trainee candidates. Building upon the training material from the former years, which was primarily based on declarative and procedural information security knowledge, we were able to design and conduct three different kinds of training sessions. While the material for training group C only builds upon declarative and procedural security knowledge, the material for training groups A and B received additional deterrence and vulnerability arguments, respectively. A detailed description of the training and the content of each training group can be found in Appendix A. The HR department identified 109 employees as training candidates. These candidates were randomly assigned to one of the three training groups and invited for training sessions. In the second step, the on-site training sessions were conducted. Due to scheduling constraints, 21 participants were unable to attend the training. In the third step, we measured training effectiveness at different
points in time. At the end of the training sessions, each trainee filled out a questionnaire capturing demographics, control variables, course feedback, and expected information security behaviour. The employees were asked to respond as realistically as possible, and it was acknowledged both verbally and in written form that the evaluation would be carried out anonymously. Information security behaviour in terms of the clean desk policy was gathered twice: one week and three weeks after the final training. Information security behaviour in terms of the email policy was gathered around two weeks after the last training session. This involved sending a spear phishing email to all trainees and counting how often participants clicked on the link within. Participants than received a warning message and information on how they could have identified the mail as malicious.

Appendix B. Training design and content
In cooperation with the company’s information security management, we identified three critical information security areas: password policy, clean desk policy, and email policy. Due to recent attacks on the company, spear phishing was identified as the primary concern regarding the email policy. We prepared training material imparting policy regulations and procedural knowledge, including instructions on how to create secure passwords, an introduction to the company’s password-management tool, and procedures for identifying and handling spear phishing emails. The training material was extended with elements emphasizing the personal and job relevance of ISP compliant behaviour. For personal relevance, this included elements underlining sanctions for non-compliant behaviour, such as fines, disciplinary actions, and peer disapproval as well as references to law violations. For work relevance, this involved arguments highlighting the company’s vulnerability to the security threat vectors if employees fail to behave in accordance with security regulations. This included
vulnerabilities enabled by weak passwords, true stories of document theft, and the high
and increasing number of phishing attacks. The arguments were supplemented with
threats to the employees’ work contexts, such as losing self-elaborated project files,
facing work impediments due to stolen notebooks, or encountering threats for the whole
company through phishing mails. Each training session was scheduled for 1.5 hours.

The training design, its content, and the content’s allocation to the training groups is
depicted in the following table.

<table>
<thead>
<tr>
<th>#</th>
<th>Area</th>
<th>Goal</th>
<th>Excerpts from training content</th>
<th>Tg A</th>
<th>Tg B</th>
<th>Tg C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Password policy</td>
<td>K</td>
<td>Introduction; examples for password security; policy regulations for password strength, password sharing, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>Password policy</td>
<td>D</td>
<td>Explanation that intended or negligent violations can lead to disciplinary sanctions or fines (with a reference to German laws)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Password policy</td>
<td>V</td>
<td>Presentation and discussion of hazardous situation for the work context; example demonstrating how easily unsecure passwords can be attacked</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>Password policy</td>
<td>K</td>
<td>Explanation of detailed procedures for creating secure but easy to remember passwords</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>Password policy</td>
<td>K</td>
<td>Introduction of the company’s password-management tool and practical examples of how and why to use it</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>Clean desk policy</td>
<td>K</td>
<td>Introduction; policy regulations; procedures for screen logging, using the notebook lock, handling of confidential information, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>Clean desk policy</td>
<td>D</td>
<td>Indication of the fine for a lost laptop due to negligence; pointing out that colleagues judge you according to the orderliness of your desk, etc.</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Clean desk policy</td>
<td>V</td>
<td>Presentation and discussion of actual intranet messages that report an increased loss of IT devices and documents due to insecure behaviour, burglary, theft, etc.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Spear phishing</td>
<td>K</td>
<td>Introduction; reference to the “usage of communication services” policy; introduction to spear phishing; example of spear phishing emails</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>Spear phishing</td>
<td>D</td>
<td>Disclosure that log files allow for tracing back misbehaviour, disciplinary consequences are likely in case of non-compliance, etc.</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Spear phishing</td>
<td>V</td>
<td>Presentation and discussion of information showing that 42% of employees in the energy industry have been attacked with phishing emails; threat of phishing rises</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>Spear phishing</td>
<td>K</td>
<td>Explanation of how spear phishing mails can be detected; explaining what should be done in case of a phishing email (incident response)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>13</td>
<td>Data protection*</td>
<td>K</td>
<td>Introduction; German and European laws (including new requirements of the General Data Protection Regulation) and regulations of the company; procedures on how to handle personal data, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: K = ISP knowledge; D = deterrence arguments; V = vulnerability arguments; Tg A = Training group A – training with deterrence arguments; Tg B = Training group B – training with vulnerability arguments; Tg C = Training group C – baseline training. * This element was supplementary to the security training due to company requirements but has no further effect on this research.
Appendix C. Measurement of variables and questionnaire scales

Intended ISP behavior and ISP knowledge. In ISP compliance studies, we find two widely applied approaches for measuring behavior. The behaviorally anchored approach aims to capture the behavior of a real actor within her/his own context, while the scenario-based measurement sets an individual in a hypothetical situation (Moody et al., 2018). The behavior-based approach measures behavior in a real context, questioning respondents in relation to their specific organizational situation. It therefore has a high level of external validity. In contrast, the scenario-based measurement describes an imaginary situation, with respondents being asked how they would act if the scenario were real. This approach allows the researcher to better specify the context under study. Moreover, scenarios circumvent the potential bias that can result from socially desirable answers; this poses a particular threat in ISP policy studies measuring deviant behavior (Chen et al., 2013; Moody et al., 2018). We decided to implement both approaches as measures for expected behavior. We used a two-item scale from Bulgurcu et al. (2010) to measure “intention to comply with the ISP.” Furthermore, we assessed specific ISP behavior relating to the three policies detailed in the training using three corresponding hypothetical scenarios. The first scenario referred to screen locking: A line manager asks the employee not to lock his screen when leaving the computer, arguing that this helps other colleagues to easily proceed with the work. The second scenario related to passing on login data: A colleague asks the employee who is on a business trip if s/he can pass on her/his credentials, claiming that this can save a lot of time for the company. The third scenario describes an internal mail from the CIO that asks the recipient to type in her/his credentials on an attached, external link. At a second glance, it becomes obvious that this is a spear phishing mail. For all three scenarios, we decided to use one-item scales for the scenario-based measurement. The item is derived from Siponen and Vance (2010) and asks whether the respondents would behave similarly to
the hypothetical characters. One item was adapted from Bulgurcu et al. (2010) for perceived ISP knowledge, measuring the degree of knowledge regarding information security policy, procedures, and guidelines. High factor loadings (> .95) of the items with similar scales across different studies (D’Arcy et al., 2009; Bulgurcu, 2010; Moody et al., 2018) led us to conclude that one-item solutions for situational ISP compliance behavior and ISP knowledge are appropriate for our study context. The questionnaire items can be found in the following table.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Label</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISP knowledge</td>
<td>PIK01</td>
<td>I know and understand the rules, procedures, and guidelines prescribed by the ISP of my organization.</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td>Situational ISP compliance intention</td>
<td>SVI01</td>
<td>What is the chance that you would do what Mr. Nagel did in the described scenario? (Refers to the clean desk policy)*</td>
<td>Siponen and Vance (2010)</td>
</tr>
<tr>
<td></td>
<td>SVI02</td>
<td>What is the chance that you would do what Mrs. Nuss did in the described scenario? (Refers to the password policy)*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SVI03</td>
<td>What is the chance that you would do what Mr. Stauzebach did in the described scenario? (Refers to the spear phishing scenario)*</td>
<td></td>
</tr>
<tr>
<td>General ISP compliance intention</td>
<td>GCI01</td>
<td>I intend to comply with the requirements of the ISP of my organization in the future.</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td></td>
<td>GCI02</td>
<td>I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.</td>
<td></td>
</tr>
</tbody>
</table>

Note: All scale items were translated from English to German. * Reverse coded since the characters in the scenario decide to violate the policy.

**Actual behavior.** A spear phishing campaign was conceived to measure actual behavior. A spear phishing mail was designed according to the trained procedures and sent to all training participants. Recipients were asked from the alleged CIO of the company to click on a link in the email. The variable *clicked on spear phishing link* counts how many participants of each training group clicked on the link in the email. For the clean desk control, the offices of the training participants were checked twice, one week and three weeks after the training. The variable *confidential information accessible* is a binary measure indicating whether internal documents were freely accessible in the offices.