6-18-2022

How Employees Learn Information Security Policy Compliance Behavior: Toward a Social Learning Perspective

Sebastian Hengstler
Chair of Information Security and Compliance, s.hengstler@stud.uni-goettingen.de

Natalya Pryazhnykova
University of Göttingen, pryazhnykova@gmail.com

Stephan Kühnel
Martin Luther University Halle-Wittenberg, stephan.kuehnel@wiwi.uni-halle.de

Recommended Citation

Hengstler, Sebastian; Pryazhnykova, Natalya; and Kühnel, Stephan, "How Employees Learn Information Security Policy Compliance Behavior: Toward a Social Learning Perspective" (2022). *ECIS 2022 Research Papers*. 85.
https://aisel.aisnet.org/ecis2022_rp/85

HOW EMPLOYEES LEARN INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR: TOWARD A SOCIAL LEARNING PERSPECTIVE

Research Paper

Sebastian Hengstler, University of Goettingen, Goettingen, Germany, s.hengstler@stud.uni-goettingen.de

Natalya Pryazhnykova, University of Goettingen, Goettingen, Germany, pryazhnykova@gmail.com

Stephan Kuehnel, Martin Luther University Halle-Wittenberg, Halle (Saale), Germany, stephan.kuehnel@wiwi.uni-halle.de

Abstract

Information security attacks typically exploit the weakest link in the chain, which is in most cases is the IT end user at the workplace. While great strides have been made in understanding and explaining information security behavior, little is known about how such behavior is acquired by individuals in the first place. This research approaches the phenomenon through the lens of social learning theory. We argue that a new employee's behavior is initially learned through differential associations within the social network, rather than through knowledge of formal policies and associated sanctions. We used a scenario-based experimental approach and collected data from new employees with five years or less of work experience. Our results show that employee's behavior changes over time. Reinforcement through sanctions becomes more important in the maintenance phase, while imitation of others becomes less relevant.

Keywords: Social Learning; Information Security; Compliance Behavior, Information Security Policy Compliance.

1 Introduction

A key instrument for achieving information security in organizations is an information security policy (ISP). ISPs encompass a set of rules and guidelines related to the processing and usage of information within an organization's authority (Baskerville and Siponen, 2002). Following recommendations in the best practice literature, organizations often implement a wide range of education and control mechanisms to motivate employees to follow their ISPs (Cram et al, 2019). However, evidence from research regarding such measures' efficiency has been unanimous, and non-compliance with ISPs remains one of the significant challenges for information security management (Trang and Brendel, 2019).

Research has adopted several perspectives to explain this phenomenon of non-compliance, often building models upon theoretical lenses, such as rational choice theory (Bulgurcu et al, 2010a; D'Arcy and Lowry, 2019; Herath and Rao, 2009), protection motivation theory (Menard et al, 2017; Posey et al, 2015), or the theory of planned behavior (Humaidi and Balakrishnan, 2018; Ifinedo, 2012). While these research stream has made significant progress in explaining employees' non-compliance with ISPs, there is still little known about the initial acquisition of ISP compliance behavior (Willison et al, 2016). We understand the initial acquisition of ISP compliance behavior as the process in which definitions (i.e., attitudes) are learned as a function of both formal and social cues, similar to the research of Sun (2013) and Darban and Polites (2020) in the context of technology adoption behavior. This learning refers to individuals, who have only a little or no prior experience with ISP related behaviors in their organization, and their positive attitude regarding ISPs are not yet strongly defined (Hengstler et al, 2021). However, it is precisely this initial learning process that is said to be important (Willison et al, 2016). From existing research, we can see that such aspects as attitudes, social values and norms are important elements for achieving ISP compliance behavior (Cram et al, 2019). These descriptive characteristics of an employee are learned in the professional environment mainly through social interactions, such as imitating the behavior of other employees (Hengstler et al, 2021). New employees with little professional experience, in particular, are still at the beginning of this learning process and their definitions (e.g. attitude, norms and values) towards their work environment that could influence ISP compliant behavior are not yet properly developed. However, this initial situation poses a high risk in practice, if, for instance, these new or less experienced employees do not adhere to ISPs and cause security breaches, such as identity theft or a data leak, because they either behave unintentionally non-compliant according to their organizations ISPs or take the wrong premises as a basis for the evaluation of possible security threats (Johnston et al, 2019).

A better understanding about the initial learning of information security behavior is crucial for several reasons. Firstly, initial learning and adopting compliance behavior is just as important as continued ISP compliance behavior, because attackers usually target the weakest link in the security chain (Ifinedo, 2014, Willison et al, 2016). Secondly, the research emphasizes the difficulties of altering behaviors after behavioral patterns become routinized (Vance et al, 2012). Thirdly , the phenomenon of non-compliance at the initial learning and adoption stage has certain characteristics that are poorly explained by current. theories. For example, the rational choice theory assumes at least a high degree of information transparency (Bulgurcu et al, 2010a). However, new employees usually have a lack of access to practical knowledge regarding the likelihood of how non-compliance is being detected. Finally, the social context in which behavior learning usually takes place often plays just a minor or side role in current research (Hengstler et al, 2021). While ISP studies that draw upon the theory of planned behavior typically include a concept of subjective norms (Herath and Rao, 2009) or normative beliefs (Bulgurcu et al, 2010b), this idea, instead, refers to a broad definition of organizational norms and does focus on the process of learning. However, research on learning generally acknowledges the importance of social embedding in a group of significant others when learning a new behavior (Feldmann et al, 2017).

Therefore, this research aims to explain differences in the process of learning ISP compliance behavior. We concentrate on the initial learning process for employees who are new in an organization and only have a few years of work experience (Willison et al, 2016). We borrow from social learning theory with a focus on Akers et al. (1989) interpretation of differential associations (DA) in criminology and deviant behavior. In doing so, we plan to contribute to current literature in extending the view on the acquisition of behavior through social learning in an early adoption stage. Instead of considering the social context as a broad definition of organizational norms, such as those incorporated in frequently used theories in information security research (e.g., the theory of planned behavior), we explain how ISP compliance behavior is learned through an individual’s social learning environment (Hsu et al, 2015).

The results of this article show how information security compliance behavior (e.g., of knowledge workers), which is constantly gaining importance in the context of digitalization and digital technologies, is learned in organizations. The focus is on the socio-technical context with regard to the ISP of an organization and the learning effect of young employees through social interactions with colleagues. Our results show that through the social elements described in the social learning theory, it is possible to learn and anchor knowledge about correct behavior regarding information security in an organization

The rest of the paper is structured as follows. In section 2, we review the social learning theory and explain its components. In section 3, we explain our research model, including social and formal cues on non-compliance behavior. We conclude section 3 by explaining the moderating influence of job tenure between social and formal cues on non-compliance behavior. We explain our research method of a scenario-based full factorial survey method in section 4 and provide information about our data analysis and results in section 5. We provide a discussion of our results in section 6, including implications for practice and further research as well as limitations of our study. The paper concludes in section 7.

2 Reviewing Social Learning Theory

Our aim in this study is to better understand how ISP compliance behavior is initially learned and later maintained. The research model is primarily informed by the social learning theory and the social learning process. We will, therefore, first review primary concepts of social learning theory. Building upon this foundation, we will then derive our research model. Burgess and Akers' (1966) social learning theory has its roots in criminology, sociology, and psychology. The theory describes how deviant behavior, like any other behavior, is learned through social interactions. Research provides empirical support for the basic concepts and predictions of various deviant behaviors, such as drug use, partner violence, or academic dishonesty (Cochran et al, 2017; Pratt et al, 2010). The theoretical premises of social learning also found wide practical application in the development of prevention programs to, e.g., reduce juvenile delinquency and victimization, or adolescence misbehavior (Nicholson and Higgins, 2010). Social learning theory, as refined in Akers (1989), integrates two theoretical lenses: from DA and operant conditioning. DA theory argues that criminal behavior is learned in interaction with others (Akers et al, 1989). This learning includes both techniques of committing the crime and motives, rationalizations, and attitudes in regard to criminal behavior. Operant conditioning argues that behavior is acquired through direct conditioning, i.e., when an individual makes an association between a particular behavior and a corresponding consequence (Skinner, 1938). Social learning theory adds to this perspective that behaviors can also be learned by observing others (Bandura, 1963). Building upon these theoretical lenses, Burgess and Akers formulate a learning process of deviant behavior that includes four main concepts (Burgess and Akers, 1966). The basic premise is that both conforming and non-conforming behavior are acquired, maintained, and changed by interacting with others. In other words, whether people show conforming or non-conforming behavior depends on conforming or non-conforming directions of social influences.For our research, we borrow three core concepts from social learning theory, i.e., DA, imitations (IM), and differential reinforcements (DR). Firstly, the concept of DA emphasizes the importance of peers for learning new behavior. DA refers to the definitions (i.e., attitudes) and behaviors one is exhibited within an individual's social network. Associations differ, e.g., in terms of frequency, duration, intensity, and priority. Social learning theory posits that the stronger the association, the more influential it is on shaping one's definitions and behaviors. Such a network can include relationships with direct team colleagues, specific members from project teams, or friends across departments when translated into information security in an organizational setting (Pratt et al, 2010). One's evaluation of ISP deviance behavior is shaped by their deviance definitions as favorable or unfavorable behavior. Secondly, IM refers to the notion that individuals engage in behavioral patterns observed in others. Whether a behavior is imitated, it depends on the observed consequences, the model's characteristics, and the association with the model. Moreover, modeling others' behavior is particularly important in the first commission of the act as one own's definitions of the behavior are weak, and consequences for the deviance have not been experienced (Akers et al, 1989). Finally, DR refers to the process by which individuals anticipated the consequences of a specific behavior. In general, this evaluation process can include past, present, and anticipated future rewards or punishments (Akers et al, 1979). The notion of learned consequences borrows from operant conditioning theory. Organizational information security and formal reinforcements can include monetary fines, rewards, or disciplinary warnings (Yang and Johnston, 2019).

While social learning theory, as refined in Akers et al. (1989), is widely used in criminology research, only few studies have used this lens to explain information security-related behaviors. The construct of deviant behavior considered in social learning theory was transferred to ISP related behavior and referred to as non-compliance behavior. For instance, Skinner and Fream (1997) explore computer crime among college students using social learning theory. Their results underline the importance of DA and IM of peer behavior, and definitions for predicting different types of illegal access to computers and data modifications. Hinduja and Ingram (2009) study the role of offline and online peers in predicting music piracy. They find evidence that the behavior of real-life peers, online peers, and online media influences delinquency (Hinduja and Ingram, 2009). Warkentin et al. (2011) study self-efficacy in the context of information privacy compliance. Their results show that an informal learning process in terms of situational support, vicarious experiences, and verbal persuasion drives self-efficacy, which shapes an employee's compliance behavior. Hengstler et al. (2021) analyze the influence of individual cultural values on how do employees learn security behavior. Although current research has made promising indications regarding the applicability of the concepts of social learning theory in non-compliant security behaviors, no study examines, how initial behavior is learned. In this study, we adapt social learning theory to our context of how employees acquire information security behavior and theorize how security behavior is initially learned.

3 Research Model

The research model consists primarily of mechanisms adapted from the social learning theory and the social learning process. The model explains intentions to violate ISPs. Table 1 gives an overview of the social learning theory's mechanisms used in this research paper, their description, and their use in our research model. Furthermore, we use the theories for hypothesis development.

Social Learning Theory	**Description**	**Research Construct**
Differential reinforcement (DR)	DR refers to the balance of anticipated or actual rewards and punishments that follow or are consequences of behavior.	Formal cues (sanctions)
Differential association (DA)	DA refers to the direct association and interaction with others who engage in certain kinds of behavior or express norms, values, and attitudes supportive of such behavior, and the indirect association and identification with more distant reference groups. The groups with which one is in differential association provide the major immediate and intermediate social contexts in which all social learning mechanisms operate.	Social cues (differential association)
Imitation (IM)	IM refers to the engagement in behavior after the direct or indirect observation of similar behavior by others.	Social cues (Co-worker behavior)
Non-Compliance behavior (NCBE)	NCBE refers to the behavioral intention to deliberately violate rules that are prescribed by the organization.	Intention to violate ISP
Learning process	The learning process includes social learning concepts defining a set of variables that are all part of the same underlying process that is occurring in each individual's learning history (both learning from and influencing others), in the immediate situation in which an opportunity for a crime arises, and in the broader socio-structural context (both at the meso and macro-levels). The social learning process is dynamic and involves reciprocal and feedback effects.	Job tenure

Table 1. Definition of research constructs.

3.1 The Influence of Social Cues on Information Security Policy Compliance Behavior

Co-worker behavior refers to an employee's observation of a co-worker's actions and attitude about ISP violations. In line with social learning theory, we argue that non-compliance behavior is learned by imitating others' behavior. In daily working routines, project-related collaborations, or just by accident, employees are exposed to different degrees of compliant and non-compliant co-worker behaviors (Sun, 2013). The effect of observing does not only enable the employee to learn the techniques which might be required to perform the non-compliance but also shapes their definition of what is regarded as good or bad behavior. This perspective is consistent with studies that cast co-workers' behaviors as a descriptive norm (Cheng et al, 2014, D'Arcy and Lowry, 2019). Moreover, motives and rationalizations for non-compliance behavior might be learned through observation. An employee who observes ISP non-compliance behavior of other colleagues thus might be more willing to engage in non-compliance (Lembcke et al, 2019). Accordingly, we posit that:

Hypothesis 1 (H1): *Co-worker non-compliance behavior has a positive effect on an employee's intention to violate the ISP.*

DA refers to different levels of relationship strength an individual can have with other groups of people. DAs can be manifested in different levels of frequency, duration, priority, and intensity of interaction. For instance, an employee may have only casual work contact with colleagues from the human resources department. Thus, the association with this group can be labeled as low. In turn, the employee might have regular contact as well as time-consuming, and intensive exchanges in project meetings with colleagues from the research and development department. This association can accordingly be labeled as high. DAs are important for the learning of non-compliance behavior because learning of deviance occurs in personal groups. Individuals are more likely to accept others' evaluations or definitions and imitate their behaviors if they exhibit a close association with them. For example, Akers and Lee (1996) were able to predict an individual's smoking behavior according to DAs by considering the friends, who are being known for smoking the longest, the friends with whom one is most often associated, and the best friends. Thus, we posit:

Hypothesis 2 (H2): *The effect of co-worker non-compliance behavior on the intention to violate the ISP is higher if the DAs between the employee and the co-worker is high.*

3.2 The Influence of Formal Cues on Information Security Policy Compliance Behavior

A common measure for ensuring that employees adhere to ISP regulations is coercive control through a set of formal cues (Cheng et al, 2013). This typically includes the implementation of deterrence measures, which organizations deliver through disciplinary sanctions such as warnings, fines, demotions, and dismissals (D'Arcy et al, 2009; Herath and Rao, 2009). The underlying rationale of sanctions as a formal mechanism to control behavior already finds some application in ISP compliance research (Trang and Brendel, 2019). Through the lens of the social learning process, formal sanctions display a DR. If an individual anticipates negative consequences related to non-compliance behavior, the employee is less likely to reveal it. A typical example for high sanction could be a job termination and a low sanction example could be a warning or a small fee (Pratt et al, 2006). While the consequences draw on a formal structure of regulations, the learning of consequences can be vicarious. A non-complying individual may not necessarily experience sanctions themselves. The peer group can also be seen as a source of information for assessing consequences. The knowledge of formal sanctions and the evaluation of the consequences shapes an individual's learning process. Accordingly, we posit that:

Hypothesis 3 (H3): *Sanctions (formal cues) related to ISP non-compliance have a negative effect on an employee's intention to violate the ISP.*

As noted earlier, we interpret co-worker behavior as an important social source for informal learning. Sanctions, as coercive control, regulate compliance through precise control. Both provide information for shaping the learning process. However, they do not necessarily provide conforming cues. This is the case for an individual who might be aware of punishments related to non-compliance and, at the same time, observes that peers behave differently. We argue for an interaction between these contradicting cues. The information gained from formal cues is more explicit and objective than social cues that are distorted by the sources' own bias and opinion (Morrison, 1993). Individuals thus solve contradicting information by devaluing the social cue. Accordingly, we posit that formal sanctions diminish the effect of co-worker non-compliance behavior.

Hypothesis 4 (H4): *The effect of the observed co-worker non-compliance behavior on the intention to violate the ISP is lower if an employee is aware of sanctions (formal cues).*

3.3 The Moderating Influence of Job Tenure Between Social and Formal Cues on Information Security Policy Compliance Behavior

Social learning theory posits that individuals start to acquire new behavior through observation and imitation. Building upon the subsequent experiences of positive or negative consequences, people form their attitudes regarding what is good or bad. When a behavior is maintained, imitating others in one's peer group becomes less important (Akers et al, 1979). This perspective of social learning fits with insights from research on newcomers about organizational socialization and temporal changes. Hamilton et al. (1980) suggests that, in the first stage, newcomers are more concerned about fitting in socially and, later, they become more concerned about how well they are performing. We refer to newcomers as employees with no more than 5 years of professional experience (Hamilton et al, 1980). Translated to the context of ISP compliance behavior, this suggests that social and formal cues play a particular role for newcomers. As definitions of ISP compliance behavior as acceptable or unacceptable are weak at the initial acquisition stage, they are more influential in shaping a newcomer's behavior. In turn, when definitions become more stable at a later stage of tenure, social and formal cues become less important. Following this rationale, we argue that:

Hypothesis 5 (H5): *The effect of the observed co-worker non-compliance behavior on intention to violate the ISP is smaller for employees with longer job tenure.*

Hypothesis 6 (H6): *The effect of sanctions on the intention to violate the ISP is higher for employees with longer job tenure. In conclusion, the explained theoretical mechanisms and the derived hypotheses lead to the research model as shown in Figure 1.*

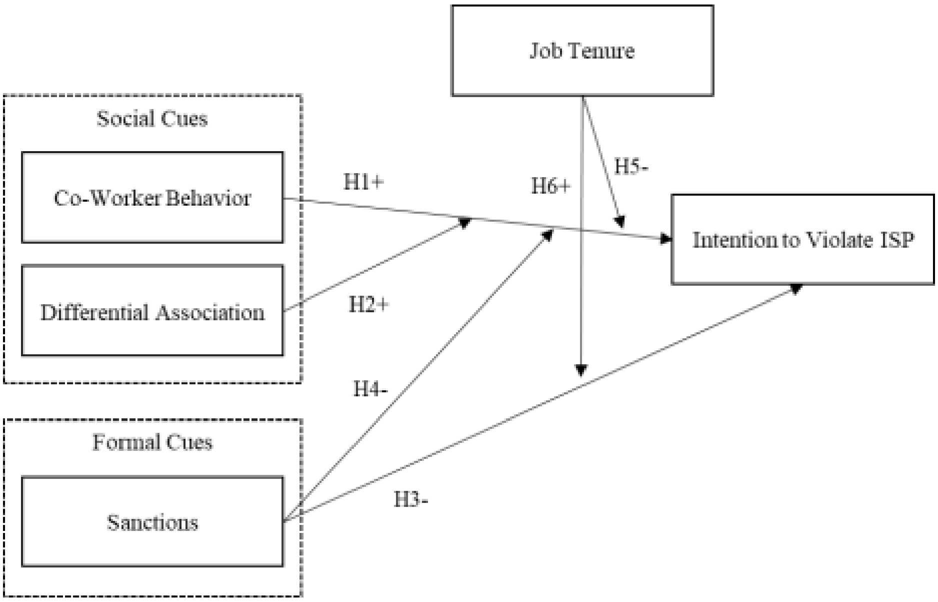

Figure 1. Research model on information security compliance behavior.

4 Method

To test the research model, we applied a scenario-based full factorial survey method. Our approach follows a mixed 2 x 2 x 3 x 2 experimental research design. This kind of study design already found applications in information security behavior (Johnston et al, 2016). The scenario-based measurement describes a hypothetical situation, with respondents being asked, how they would act if the scenario was real. This approach has two primary advantages (Moody et al, 2018). First of all, it allows the researcher to better specify the context under study. Second, scenarios circumvent the potential bias resulting from socially desirable answers; this poses a particular threat in ISP policy studies measuring non-compliance behavior. To test the influence of the independent variables, we decided to implement an experimental scenario-based survey design. Each scenario includes a different manipulation of the used independent variables. The variables are operationalized as factors with different levels. A level comprises a statement that enhances the context of the scenario in the sense of the variable. Based on this operationalization, the scenarios are then derived for all factor combinations, i.e., factors and levels. Participants in the survey then read a scenario and responded accordingly. In contrast to correlational research designs, the randomized allocation of groups of scenarios to participants and the randomization of scenarios within a group of scenarios allowed us to control for unobserved variables and spurious correlations.

4.1 Instrumentation and Pretest

Based on the scenario design, we operationalized our research variables. We decided to implement two typical base scenarios to capture non-malicious behavioral responses for the dependent variable intention to violate ISP. Both scenarios are based on a fictional employee (Julia), who works at a company's accounting unit. The first scenario describes a situation in which sensitive information on a USB stick are not encrypted and, thus, violates the internal ISP. The second scenario describes a situation in which a person does not logoff the account from the computer and, thus, violates the internal ISP. The intention to violate the ISP is operationalized with two items (Moody et al, 2018). The items measure the likelihood that the respondent would act in the same way as Julia did. The independent variables were operationalized as factors. For the first variable, sanctions, a factor was derived and varied at two levels, i.e., low and high sanctions. The second and third variables, IM and DA, were implemented with the factor observed behavior and administered with three levels, i.e., no peer behavior, non-compliant behaviors of colleagues, and non-compliant behavior of close peers. The third factor, job tenure, varied at two levels describing either a character who recently started in his/her first job (i.e, a new employee) or a character who already worked for five years in that company (i.e., a junior employee). In total, the research design, including the two base scenarios, produced 24 factor combinations. The instrumentation is depicted in table 2.

Variable	Factor	Level	Coding
Sanctions	Sanctions	Low	0
		High	1
Co-worker behavior	Observed behavior	No peer behavior observation	0
		Observation of non-compliant behavior of colleagues	1
		Observation of non-compliant behavior of close peers	1
Differential association	Observed behavior	No peer behavior observation	0
		Observation of non-compliant behavior of colleagues	1
		Observation of non-compliant behavior of close peers	1
Job tenure	Job Tenure	New employee	0
		Junior employee	1
Scenario	Scenario	Screen locking	0
		USB stick encryption	1

Table 2. Instrumentation of factor combinations.

In scenario-based research designs, it is of utmost importance that the hypothetical scenarios are both relevant and realistic (Siponen and Vance, 2014). When designing the scenarios, we thus extensively examined prevailing practices in information security and the existing literature. Moreover, we conducted a pretest and interviewed eight experts on research design and four experts on information security. Minor changes were made in the wording of the scenarios. Ultimately, the scenarios were deemed to be realistic and relevant. As a post hoc measure, we also included two items to check for the realism of the scenarios. The used items and scenarios are listed in table 3.

Construct	**Item / Scenario**
Intention to Violate ISP	I could imagine acting like Julia in this situation.
	The likelihood that I would do the same in Julia’s situation is high.
Formal Cues	The probability that Julia will be caught for not complying with safety regulations is high
	Julia is likely to face heavy sanctions.
	Following the safety rules will take a long time.
Social Cues	It is important to Julia how her colleague Lukas feels about her
	It is important to Julia how her colleague feels about her.
	It is important to Julia how her colleagues feel about her.
	Lukas is an important reference person for Julia.
	The colleague is an important reference person for Julia.
	The colleagues are important reference persons for Julia.
Realism Check	Putting myself in Julia’s situation was easy
	The scenarios presented seemed realistic to me
Scenario 1	Julia recently finished her studies and started her first job in the controlling department of a company (T0) (Julia has been working in the controlling department of a company for 5 years (T5)). In this job she works daily with sensitive data. For the security of the information on her computer, Julia was told by the IT manager on the first day that she had to log off from her computer every time she leaves her workplace, no matter how short it may be. **[…]** Failure to comply will result in a warning letter or a loss of salary. **[…]** Julia is not aware that there have ever been any consequences for disregarding this instruction. Since Julia has to leave the computer more often during the day to talk to colleagues, logging on and off takes a lot of time throughout the day. **[…]** Lukas, who introduced Julia to the new job, has meanwhile become a friend. She notices that Lukas does not log off his computer every time, only for lunch and after work. **[…]** Julia notices that her colleague does not log off his computer every time, only for lunch and after work. **[…]** Julia does not know how her colleagues deal with the safety regulations. She decides to violate the security regulations and not to log off from her PC.
Scenario 2	Julia recently finished her studies and started her first job in the controlling department of a company (T0) (Julia has been working in the controlling department of a company for 5 years (T5)). In this job she works daily with sensitive data. For the security of the sensitive information, Julia was informed by the IT manager on the first day that she always had to encrypt data that she provided to colleagues using a USB stick. **[…]** Failure to comply will result in a warning letter or a loss of salary. **[…]** Julia is not aware that there have ever been any consequences for disregarding this instruction. Since Julia very often has to make data available to colleagues with the help of a USB stick in her job, encryption takes a lot of time throughout the day. **[…]** Lukas, who introduced Julia to the new job, has now become a friend. Julia notices that Lukas does not encrypt the data on the stick. **[…]** Julia notices that her colleague does not encrypt the data on the stick. **[…]** Julia does not know how her colleagues deal with the safety regulations. Julia decides to violate the security regulations and not to encrypt the USB stick.

Table 3. Used items per construct.

4.2 Power Analysis, Sample Characteristics, Test for Realism and Manipulation Check

Based on the operationalization of the research variables in a 2 x 2 x 3 x 2 factor structure, we derived 24 different scenarios. It was decided to receive behavioral responses using a fractional design. In a fractional design, respondents receive multiple scenarios (Siponen and Vance, 2014). Fractional designs are standard in scenarios-based studies to increase the ability to manipulate critical variables. However, too many scenarios can lead to an overload of information and fatigue (Weber, 1992). Thus, we decided to specify the external conditions, i.e., the two scenarios and the two levels of sanctions, as between-subject factors, and the behavioral cues, i.e., IM and DA, and job tenure as within factors. Accordingly, each participant was randomly assigned to one of four groups (either the USB encryption or the notebook-locking scenario, and either the low or high sanctions treatment). The test person then responded to six scenarios that differed in terms of colleagues’ observed behavior and job tenure. To control for possible order or carryover effects, we randomized the order of the scenarios presented to the respondents. In order to determine an acceptable sample size, we conducted an a priori power analysis. A power analysis with G*Power 3.1.9.2 assuming a small effect size reveals a lower bound of at least 132 participants (multiple linear regression for a fixed model and significant single regression coefficients, $f = .10$, $\alpha = .05$, power = .95, 5 predictors). Our experiment’s target group consisted of employees that reveal to have similar characteristics as our hypothetical character from the scenarios, i.e., a newcomer with only little to medium job tenure (maximum 5 years). This ensures a higher congruence between the test participants and the persons described in the scenarios, as the duration of the employment varied between 0 and 5 years. In order to reach the target group, the link was mainly distributed via student university groups on Facebook. Since the survey was conducted in German, the focus lied on German university groups. As an incentive, five €20 gift cards were raffled among the participants. A total of 530 persons participated in the survey, 312 of whom completed it.

To ensure data completeness and consistency, only fully completed questionnaires were included in the further analysis as well as responses with the appropriate job tenure. There were no restrictions in the industry. The average age of participants in the sample was 24.7 years, with 39% female and 61% male. Of the respondents, 1% stated that their highest level of education completed was middle school or equivalent, 25% earned a high school degree or equivalent, 57% held a bachelor’s degree or equivalent, and 17% held a master’s degree or equivalent. The average job tenure was 2.7 years. Using a multi-group analysis, we examined our control groups age, gender, work experience, and educational background and found no significant differences between our treated and control groups. A summary of the sample characteristics is shown in table 4. Table 5 shows the results of the data collection per scenario.

Demographics	**Numerics**	**Total count**	**Demographics**	**Numerics**	**Total count**
Gender	Female	196 (63%)	Education	Economics	96 (31%)
	Male	114 (37%)		Teaching	39 (13%)
	Other	2 (1%)		Natural Sciences	31 (10%)
Age	≤18	20 (6%)		Social Sciences	26 (8%)
	19-21	110 (35%)		Medicine	19 (6%)
	22-24	85 (27%)		Computer Science	15 (5%)
	25-27	66 (21%)		Legal Sciences	12 (4%)
	28-30	31 (10%)		Linguistics	11 (4%)
	31 or older	0		Engineering Sciences	10 (3%)
Academic degree	High School Grad.	188 (60%)		Politics	10 (3%)
	Bachelor	81 (26%)		Other	43 (14%)
	Master	29 (9%)	Work experience	Less than 1year	110 (35%)
	Other	14 (4%)		1-2 years	117 (38%)
				3-4 years	49 (16%)
				5 years	36 (12%)

Table 4. Descriptive sample statistics.

Scenarios	**Logoff Screen**	**Encryption**	**Total**
Sanctions: HIGH	70 (22,4%)	77 (24,7%)	147 (47,1%)
Sanctions: LOW	82 (26,3%)	83 (26,6%)	165 (52,9%)
Total	152 (48,7%)	160 (51,3%)	312 (100%)

Table 5. Results of the data collection per Scenario.

In order to elicit valid responses in scenarios-based research, it was important for the respondents to be able to place themselves into the situation described (Weber, 1992). Therefore, we implemented an item regarding the realism of the scenarios ("I could imagine a similar scenarios taking place at work."). The average respondent reported a 5.6 on a seven-point Likert scale ranging from do not agree to agree. Moreover, we controlled for realism in our baseline model. The variable reveals to have no significant influence. We also checked whether the manipulation in terms of social cues and formal cues had the expected effects. We implemented treatment check items for each manipulation. We estimated mixed models for each item and clustered them for the individuals. As expected, we found significant differences (p < .01) for all three manipulations and thus, the scenarios are realistic.

5 Data Analysis and Results

The experimental data set contains survey data for 2112 scenarios from 312 individuals. Since the scenarios responses are not independent, and the data structure is nested, we apply hierarchical linear modeling (HLM) as shown in table 6. The scenarios responses are clustered within a Level 1 model according to the individuals at Level 2. We estimated three models to test our hypotheses. The first model estimated violation intention with controls only (model 1). The second estimation involved the direct effects of sanctions, co-worker non-compliant behavior, and co-worker non-compliant behavior with DAs (model 2). The third included the interaction effects (model 3). The first observation includes the model fit in terms of the Bayesian Information Criterion (BIC), which has improved when including the research variable (BIC of model 2 and 3 is lower than of model 1).

Variable	**Model 1**	**Model 2**	**Model 3**
Fixed effects			
Intercept	**3.422** (.346)**	**2.945** (.358)**	**2.843** (.361)**
Sanctions		-.153 (.151)	-.078 (.171)
Job Tenure		**.186** (.047)**	**.173** (.091)**
Co-worker behavior		**.540** (.057)**	**.801** (.088)**
Differential association		**.338** (.057)**	**.338** (.057)**
Sanctions x co-worker behavior			**-.345** (.099)**
Job tenure x co-worker behavior			-.199 (.098)
Job tenure x sanctions			**.309** (.093)**
Controls			
Scenario (Screen logging vs. USB-stickencryption)	**.386** (.152)**	**.383** (152)**	**.383** (.152)**
Gender	-.027 (.015)	-.031 (.152)	-.031 (.152)
Age	-.016 (.011)	-.016 (.011)	-.016 (.011)
Random effects			
Respondent (variance)	1.806	1.828	1.831
BIC	7406	7198	7193
logLik	-3680	-3561	-3547
Df	2106	2102	2099
N	934	934	934
Respondents	312	312	312

Table 6. Results of linear mixed model estimations (: significant at 0.05; **: significant at 0.01).*

This suggests that it makes sense to include research variables and interpret them. Following that model 2 suggests that direct effects are significant, it supports to include further variables of the model. Additionally, we observed that the direct effect of sanctions becomes insignificant, and the interaction terms with sanctions become significant in model 3. This indicates that the interactions are the main cause for the role of sanctions. As mentioned earlier, sanctions have no effect—only its interaction with observed co-worker behavior. The moderating effect of sanctions greatly influences the effect strength of co-worker behavior on the intention to comply with both low and high DAs (Cooper and Klein, 2018).

The first observation includes the model adaptation with respect to the BIC. This has improved with the inclusion of the research variables, as the BIC is considered that the model with the smallest value of the information criterion has a better fit than the alternative models (the BIC of models 2 and 3 is lower than that of model 1). This suggests that it is useful to include and interpret research variables.

Subsequently, model 2 shows that the direct effects of co-worker behavior with low and high DAs on intention to violate are significant, which supports the inclusion of other variables of the model. Furthermore, we observed that the direct effect of sanctions becomes insignificant and the interaction conditions with sanctions become significant in model 3.

In relation to our previously established hypotheses, we can make the following statements: Hypothesis 1 can be supported, since co-worker non-compliant behavior has a positive effect on an employee's intention to violate the ISP (significant at .01). The effect of co-worker non-compliant behavior on an employee's intention to violate the ISP was higher with a high DA than with a low one, supporting hypothesis 2 (significant at .01). We were not able to observe a direct significant effect of sanctions on the intention to violate ISP, which led to no support for our hypothesis 3. The intention to violate ISP is lower when the respondent is aware that he or she will be punished for the offence, which supports hypothesis 4. Furthermore, the job tenure positively affects the effect of sanctions and negatively co-worker non-compliant behavior, which is supporting hypothesis 5 and 6.

6 Discussion

This study addresses the gap in understanding how ISP compliance behavior is initially learned and later maintained. While the existing literature offers some approaches to describing social learning theory in criminology research, only few studies explain information security compliance behavior using social learning theory. The results of our study contribute to the information security behavior research, using social learning theory. As the results of the study show, this aspect proves to be crucial: our results suggest that compliance behavior can be learned through observation, rather than through formal mechanisms such as sanctions.

In this study, we found out that new employees imitate compliance behavior from their co-workers. This effect becomes stronger if the behavior is observed from co-workers with a close relationship. Sanctions primarily diminish the effect of imitating behavior. Surprisingly, we find no direct effect of sanctions in model 3. Our estimations show that the effect of sanctions can primarily be attributed to its moderating role as we could not observe any direct influence of sanctions on the intention to violate ISP. Our results show that sanctions rather have an influence on the imitation process of a person who observes non-compliant behavior among co-workers and plans to imitate it. However, if the imitation process reveals that high sanctions are to be expected for imitating the co- worker's non-compliant behavior, the willingness to actually violate the ISP decreases.

Our study provides a contribution to the research is in various aspects. This research aimed to explain differences in the process of learning ISP compliance behavior. In our case, this behavior is related to non-compliance to ISP's (Willison et al, 2016). We used parts of the social learning theory with an emphasis on the interpretation of Akers et al. (1989) and analyzed the effectiveness of learning mechanisms. They were characterized by formal and social cues on compliance behavior for job tenure.

Thus, we contributed to the current literature in two ways. Firstly, we extended the view on the acquisition of ISP compliance behavior through social learning in an early adoption stage of newcomers.

Within our sample, we were able to show that ISP compliance behavior is learned through an individual's social learning environment instead through formal cues. Our results indicate that formal cues, such as sanctions, rather play a moderating role in the social learning process, than directly influencing compliance behavior. Thus, we established more precise links between the social context and information security behavior (Hsu et al, 2015). Secondly, recent research provides promising evidence for the applicability of social learning theory concepts in the context of non-compliant security behavior (Lembcke et al, 2019), although there has been no study investigating the process of learning initial behavior. We adapted social learning theory to the context of initial learning of information security behavior of employees and theorized the process of how security behavior is initially learned. Especially employees with little work experience learn information security behavior from their co-workers and that this effect is more substantial when they are close to these employees.

For scientific perspective, these findings provide an important basis for taking social learning sufficiently into account in future research. Our findings also offer different implications for practice. Human resource departments, work- and organizational psychologist, pedagogical- and adult education experts can benefit from our findings and reorganize information security measures in the company, especially for new employees and colleagues with less working experience. As our results show that learning effects are usable in our context to achieve ISP compliance, experts could use our findings to define more effective information security countermeasures. Especially in our examples of screen logging or USB-stick encryption, experts could use the power of, e.g., group learning or other interpersonal learning formats to train information security compliance with rather inexperienced employees. This could be reflected, for example, in group training measures in the common social environment of a new employee concerning information security, in which he or she preferably learns together with close and experienced co-workers to achieve compliant information security behavior. Nevertheless, companies should not only control the guarantee of information security through security education, training, awareness. They should also take the effect of sanctions into account, although the results in our context show that sanctions do not have a direct effect on ISP compliance, but do have a moderating effect on the learning process. Experts should therefore take training measures and also keep sanctions noticeable for employees to strengthen the outcome of the applied information security trainings.

However, there are some limitations and a need for further research. First, our study does not provide fully generalizable results, thus requiring further investigation and follow-up studies. Researchers should use different approaches, such as considering different security threats as encryption or USB misuse, or other theoretical perspectives to analyze the problem. Secondly, we can conclude from other research (Aurigemma and Mattson, 2019; Tomasello et al, 1993) that both information security compliance behavior and social learning factors depend on contextual distinctions, such as cultural factors (Hovav and D'Arcy, 2012). This also includes our focus on the initial acquisition process of ISP compliance behavior for employees with no or only low job tenure and not at a renewal of ISP's in an organization. The acquisition process after the introduction of new ISP's in an organization should be considered in future research as well, to get a better overview about different types of social learning processes in compliance contexts. Thirdly, it should be noted that social interactions cannot only be explained by the mechanisms of social learning theory. The influence of other theories to explain social behavior, such as the theory of planned behavior including social norms, or social cues should be considered in future research. Fourthly, we did not make any differences in the industry or in the context the analysis of the social learning process of ISP compliance behavior has been employed. Future research should take a closer look at the extent to which an IT secure work environment, e.g., in a bank, has an influence on information security compliance behavior.

Despite the findings on the learning process of ISP compliance behavior among young professionals, one aspect remains open in the context of this research approach: ensuring compliance with existing information security policies by the selected senior employees within the social environment. The selection of senior colleagues to induct young professionals is important for compliance behaviors to be properly learned/conveyed in the first place. However, since we did not focus on the behavior of senior colleagues, we did not investigate this further in this study, but we see this as a research desideratum. Future research could examine this aspect, for example, in experiments with different group characteristics (e.g., colleagues who tend to engage in either compliance or non-compliance behavior).

Finally, our results show that learning about compliant behavior should be promoted, especially during job entry. Therefore, a precise design of such measures, such as security education awareness and training, should be part of future research.

7 Conclusion

With this study, we aimed to gain insights into how new employees learn ISP compliance behaviors, which is increasingly important in the context of digitization and the use of digital technologies. Drawing on social learning theory, we argued that new behaviors are learned primarily through the social environment rather than formal sanctions. Moreover, we posited that initial ISP compliance behavior is different from maintained behavior. While new employees learn through observing and imitating others, established employees also learn from reinforcements in official sanctions.

This has important implications for practice. Organizations often rely only on formal policies with sanction mechanisms that are signed during the onboarding stage. However, the (non-)application of the full range of security policies and procedures in daily behaviors might be learned on the job. Organizations should ensure that such behaviors do not become routine at this early stage. Measures to achieve this could include programs accompanying the onboarding process, such as dedicated security mentoring programs, self-reflections, or security training groups for new employees.

References

Akers, R. L. and Lee, G. (1996). “A longitudinal test of social learning theory: Adolescent smoking,” *Journal of drug issues* 26 (2), 317-343.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. and Radosevich, M. (1979). “Social Learning and Deviant Behavior: A Specific Test of a General Theory,” *American Sociological Review* 44 (4), 636–655.

Akers, R. L., La Greca, A. J., Cochran, J. and Sellers, C. (1989). “Social learning theory and alcohol behavior among the elderly,” *Sociological Quarterly* 30 (4), 625-638.

Aurigemma, S. and Mattson, T. (2019). “Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research,” *Journal of the Association for Information Systems* 20 (12), 1700-1742.

Bandura, A. 1963. *Social Learning and Personality Development*. 1st Edition. New York: Holt, Rinehart, and Winston.

Baskerville, R. and Siponen, M. (2002). “An Information Security Meta-Policy for Emergent Organizations,” *Logistics Information Management* 15 (5), 337-346.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* 34 (3), 523-548.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). “Quality and Fairness of an Information Security Policy as Antecedents of Employees’ Security Engagement in the Workplace: An Empirical Investigation*.” 43rd Hawaii International Conference on System Sciences*, 1-7.

Burgess, R. L. and Akers, R. L. 1966. “A Differential Association-Reinforcement Theory of Criminal Behavior,” *Social Problems* 14 (2), 128-147.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013). “Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory,” *Computers & Security* 39, 447-459.

Cochran, J. K., Maskaly, J., Jones, S. and Sellers, C. S. (2017). “Using Structural Equations to Model Akers’ Social Learning Theory with Data on Intimate Partner Violence,” *Crime & Delinquency* 63 (1), 39-60.

Cooper, D. T. and Klein, J. L. 2018. “Examining College Students’ Differential Deviance: A Partial Test of Social Structure-Social Learning Theory,” *Journal of Human Behavior in the Social Environment* 28 (5), 602-622.

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* 43 (2), 525-554.

D’Arcy, J., Hovav, A. and Galletta, D. F. (2009). “User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research* 20 (1), 79–98.

Darban, M. and Polites, G. 2020. “Why is it Hard to Fight Herding? The Roles of User and Technology Attributes,” *Data Base for Advances in Information Systems* 51 (4), 93-122.

D’Arcy, J. and Lowry, P. B. (2019). “Cognitive-Affective Drivers of Employees’ Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study,” *Information Systems Journal* 29 (1), 43-69.

Feldman, H. O., Dunsmoor, J. E., Kroes, M. C. W. and Lackovic, S. P. (2017). “Associative Learning of Social Value in Dynamic Groups,” *Psychological Science* 28 (8), 1160-1170.

Hamilton, D. L., Katz, L. B. and Leirer, V. O. (1980). “Cognitive Representation of Personality Impressions: Organizational Processes in First Impression Formation,” *Journal of Personality and Social Psychology* 39 (6), 1050-1063.

Hengstler, S., Pryazhnykova, N. and Trang, S. (2021). ”How do Employees Learn Security Behavior? Examining the Influence of Individual Cultural Values and Social Learning on ISP Compliance Behavior.” *54th Hawaii International Conference on System Sciences*, 4518-4527.

Herath, T. and Rao, H. R. (2009). “Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness,” *Decision Support Systems* 47 (2), 154–165.

Hinduja, S. and Ingram, J. R. 2009. “Social Learning Theory and Music Piracy: The Differential Role of Online and Offline Peer Influences,” *Criminal Justice Studies* 22 (4), 405-420.

Hovav, A. and D’Arcy, J. (2012). “Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea,” *Information & Management* 49 (2), 99-111.

Hsu, J. S. C., Shih, S. P., Hung, Y. W. and Lowry, P. B. (2015). “The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness,” *Information Systems Research* 26 (2), 282-300.

Humaidi, N. and Balakrishnan, V. (2018). “Indirect Effect of Management Support on Users’ Compliance Behavior Towards Information Security Policies,” *Health Information Management Journal* 47 (1), 17-27.

Ifinedo, P. (2012). “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory,” *Computers & Security* 31 (1), 83-95.

Johnston, A. C., Warkentin, M., Dennis, A. R. and Siponen, M. (2019). “Speak their language: Designing Effective Messages to Improve Employees’ Information Security Decision Making,” *Decision Sciences* 50 (2), 245-284.

Johnston, A. C., Warkentin, M., McBride, M. and Carter, L. (2016). “Dispositional and Situational Factors: Influences on Information Security Policy Violations,” *European Journal of Information Systems* 25 (3), 231–251.

Lembcke, T. B., Masuch, K., Trang, S., Hengstler, S., Plics, P. and Pamuk, M. (2019). “Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory.” *Twenty-fifth Americas Conference on Information Systems*, Cancun, 2019.

Menard, P., Bott, G. J.,and Crossler, R. E. (2017). “User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self- Determination Theory,” *Journal of Management Information Systems* 34 (4), 1203–1230.

Moody, G. D., Siponen, M. and Pahnila, S. (2018). "Toward a Unified Model of Information Security Policy Compliance," MIS quarterly 42 (1), 285-311.

Morrison, E. W. (1993). “Longitudinal Study of the Effects of Information Seeking on Newcomer Socialization,” *Journal of applied psychology* 78 (2), 173-183.

Nicholson, J. and Higgins, G. E. (2010). *Social Structure Social Learning Theory: Preventing Crime and Violence*. Cham: Springer International, 11–20.

Posey, C., Roberts, T. L. and Lowry, P. B. (2015). “The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets,” *Journal of Management Information Systems* 32 (4), 179-214.

Pratt, T., Blevins, K., Daigle, L. and Madensen, T. D. (2006). *The Empirical Status of Deterrence Theory: A Meta-Analysis* (15),367–395.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, L., Madensen, T. D., Daigle, L. E. and Gau, J. M. (2010). “The Empirical Status of Social Learning Theory: A Meta-Analysis,” *Justice Quarterly* 27 (6), 765-802.

Siponen, M. and Vance, A. (2014). “Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations,” *European Journal of Information Systems* 23 (3), 289-305.

Skinner, B. F. (1938). *The Behavior of Organisms: An Experimental Analysis*,. New York, Appleton-Century.

Skinner, W. F. and Fream, A. M. (1997). “A Social Learning Theory Analysis of Computer Crime Among College Students,” *Journal of research in crime and delinquency* 34 (4), 495-518.

Sun, H. (2013). “A Longitudinal Study of Herd Behavior in the Adoption and Continued Use of Technology,” *MIS Quarterly* 37 (4), 1013–1041.

Tomasello, M., Kruger, A. C. and Ratner, H. H. (1993). "Cultural Learning," *Behavioral and Brain Sciences* 16 (3), 495-511.

Trang, S. and Brendel, A. B. (2019). “A Meta-Analysis of Deterrence Theory on Information Security Policy Compliance Research,” *Information Systems Frontiers* 21 (1), 1265-1284.

Vance., A., Siponen, M. and Pahnila, S. (2012). “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory,” *Information and Management* 49 (3/4), 190–198.

Warkentin, M., Johnston, A. C. and Shropshire, J. (2011). “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention,” *European Journal of Information Systems* 20 (3), 267–284.

Weber, J. (1992). “Scenarios in Business Ethics Research: Review, Critical Assessment and Recommendations,” *Business Ethics Quarterly* 2 (2), 137-160.

Willison, R., Warkentin, M. and Johnston, A. C. (2016). “Examining Employee Computer Abuse Intentions: Insights From Justice, Deterrence and Neutralization Perspectives,” *Information Systems Journal* 28 (2), 266-293.

Yang, N. and Johnston, A. (2019) "The Application of Operant Conditioning Theory in Employees’ IS Security Behavioral Management," *ICIS Proceedings*.