WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED

Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks

Bauer, Stefan; Bernroider, Edward; Chudzikowski, Katharina

Published in:
Computers and Security

DOI:
10.1016/j.cose.2017.04.009

Published: 01/01/2017

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for published version (APA):
Bauer, S., Bernroider, E., & Chudzikowski, K. (2017). Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks. *Computers and Security*, *68*, 145 - 159. https://doi.org/10.1016/j.cose.2017.04.009

Download date: 13. Jul 2024

COMPUTERS & SECURITY 68 (2017) 145–159

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks

Stefan Bauer [a], *Edward W.N. Bernroider* [a,*], *Katharina Chudzikowski* [b]

[a] *WU (Vienna University of Economics and Business), Institute for Information Management and Control, Welthandelsplatz 1, 1020 Vienna, Austria*

[b] *University of Bath, School of Management, Bath BA2 7AY, UK*

ARTICLE INFO

Article history:
Received 24 February 2016
Received in revised form 14 March 2017
Accepted 11 April 2017
Available online 17 April 2017

Keywords:
Information security awareness
Information security awareness programs
Information security compliance
Information security policy
User perceptions
Banks

ABSTRACT

In organizations, users' compliance with information security policies (ISP) is crucial for minimizing information security (IS) incidents. To improve users' compliance, IS managers have implemented IS awareness (ISA) programs, which are systematically planned interventions to continuously transport security information to a target audience. The underlying research analyzes IS managers' efforts to design effective ISA programs by comparing current design recommendations suggested by scientific literature with actual design practices of ISA programs in three banks. Moreover, this study addresses how users perceive ISA programs and related implications for compliant IS behavior. Empirically, we utilize a multiple case design to investigate three banks from Central and Eastern Europe. In total, 33 semi-structured interviews with IS managers and users were conducted and internal materials of ISA programs such as intranet messages and posters were also considered. The paper contributes to IS compliance research by offering a comparative and holistic view on ISA program design practices. Moreover, we identified influences on users' perceptions centering on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors. Finally, the study raises propositions regarding the relationship of ISA program designs and factors, which are likely to influence users' ISP compliance.

© 2017 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Banks have been in desperate need of improving information security (IS) for decades (Baskerville et al., 2014; Goel and Shawky, 2009; Kjaerland, 2005). They operate in a complex, regulated and rapidly evolving global environment in which constantly changing or new emerging technologies are needed for conducting their operations (Goldstein et al., 2011). At the same time, financial service institutions are prime targets for crime and fraud (Norton and Walker, 2014). As a result they are increasingly threatened by data- and function-related IS risks leading to growing level of IS breaches worldwide (ORX, 2014; PricewaterhouseCoopers, 2014). There is also an

* *Corresponding author.*
E-mail addresses: stefangeorgbauer84@gmail.com (S. Bauer), k.chudzikowski@bath.ac.uk (K. Chudzikowski), edward.bernroider@wu.ac.at (E.W.N. Bernroider).

http://dx.doi.org/10.1016/j.cose.2017.04.009

0167-4048/© 2017 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

uninterrupted flow of media reports about IS breaches in banks on a global level. Only recently, more than 3.2 million debit cards issued by Indian banks were compromised (Shukla and Bhakta, 2016). The Federal Deposit Insurance Corporation (FDIC) reported to US Congress about five major bank related incidents each involving more than 10,000 data records, and previously an incident caused by a departing employee accidentally breaching the data of roughly 44,000 FDIC customers (Davidson, 2016).

Bank regulators have realized that much is at stake for banks and that professional management of IS is crucial to cope with IS risks (Hsu et al., 2013). Since the international banking regulation Basel II was enacted in Europe in 2004, measurement and quantification of operational risk, which consists of risks resulting from processes, people, and systems, is mandatory for banks (Luthy and Forcht, 2006). Particular emphasis is drawn on data and function related IT operational risk (Goldstein et al., 2011). Banks have to cover these risks by forming reserves according to the measurement approaches of operational risk (Jobst, 2007). Banks use amongst others the advanced measurement approach to calculate risk, which is based on previous loss data of the bank (Jobst, 2007). To reduce their obliged capital reserves banks are therefore interested in minimizing IS incidents in addition to avoiding reputational damage (Gillet et al., 2010). Accordingly, most prior research on IS and compliance in the context of banks has considered Basel II as the reference regulatory framework (Bauer, 2012). Other regulations, however, introduce similar requirements in terms of mitigating risks by reducing IS incidents. European (re-)insurance companies, for example, need to respond to solvency regulation (EU, 2009). The broader Sarbanes Oxley Act (SOX) also aims at IS to ensure reliable financial reports and protect shareholders from corporate fraud (US-Congress, 2002). It triggered a wave of worldwide adaptations and derivations of SOX with similar compliance requirements, e.g., the European version publicly known as EUROSOX (EU, 2006).

Besides technology, human behavior is generally seen as the biggest threat for IS (Crossler et al., 2013; Lebek et al., 2014). Users regularly cause IS incidents by volitional or non-volitional risk-taking behavior, such as careless information handling, surfing on unsecure webpages, thoughtless usage of mobile devices, or unsecure data practices (Siponen and Vance, 2010; Stanton et al., 2005). Risk-taking behavior can open further possibilities to harm the bank for internal malicious coworkers or external perpetrators (Guo, 2013). Malicious behavior and fraud, such as theft of confidential data, can be enabled by a toxic combination of risky behaviors of the staff (Warkentin and Willison, 2009). During the last decade, banks started to implement preventive controls such as information security policies (ISP), which introduce a binding standard concerning IS behaviors among all users, to reduce IS related loss incidents (Höne and Eloff, 2002). IS policies outline specific security requirements, but they do not work alone (Warkentin and Willison, 2009). Hence, organizations concentrate on fostering employee information security awareness (ISA), which is defined as "a state where users in an organization are aware of their security mission" (Siponen, 2000, p. 31). ISA is a long-standing challenge (Goodhue and Straub, 1991) and technology innovations make it harder for users to stay up to date about related new IS threats (Baskerville et al., 2014). Structured ISA programs are used by organizations to educate the employees about IS risks and how to behave to comply with the ISP (Johnson, 2006). Accordingly, such ISA programs comprise systematically planned ISA interventions, which aim to continuously transport security information to a target audience (Siponen, 2000). These ISA interventions may include intranet messages, posters, printed cups, or e-learning tutorials to increase users' ISA and to reduce volitional and non-volitional risk-taking behavior. Prior research has shown that ISA can lead to improved IS behavior and ISP compliance (Bauer and Bernroider, 2017; Bulgurcu et al., 2010; Eminağaoğlu et al., 2009), e.g., an increased protection of confidential information (Thomson and von Solms, 1998). So far, scholarly literature has discussed mostly single and neglected multi-layered ISA program designs (Kajzer et al., 2014; Shaw et al., 2009).

This study aims to address the challenge of IS management in banks to design ISA programs, and explores how users perceive program designs embedded in organization settings. Hence, we asked the following questions: How does IS management in banks design ISA programs and how such programs and their effects are perceived by users in the respective context? To answer these questions, we first draw on literature highlighting current design practices of ISA programs and several design recommendations, and how users view compliance related to the ISP. Second, a case study design, illustrating three cases, is used to present experiences of IS managers and users as to how ISP compliance is enhanced and how ISA program designs are perceived reflecting on ISP compliant behaviors. For this purpose, we analyzed responses from 10 interviews with IS managers and 23 interviews with users of the three banks. We differentiated between two groups of employees based on the rational that those groups' views on IS experiences differ. First, IS managers who manage IS or IT and, second, users who work in any business function of the respective bank. For the latter, our explorative approach focuses on individual perceptions of users centering on IS risks, their (roles) responsibilities, and how they emphasize ISP importance and knowledge, and potential non-compliant behaviors. Finally, we consolidate the results by raising propositions regarding the relationships of ISA program designs and factors which are likely to influence users' ISP compliance. In addition, the case study findings highlight the need to focus on greater attention on context sensitive designs of such programs utilizing past experiences.

The remainder of the paper is structured as follows. First, we briefly summarize previous research on the efforts of IS managers to establish IS with a focus on ISA programs and employees' views on IS and ISP compliance. Second, we introduce the research methodology and process of empirical fieldwork followed by the main results of the study. Next, we provide an in-depth discussion of the results and raise propositions for further research. Finally, we conclude the paper by summarizing the main findings and directions for further research.

2. Conceptual background

2.1. *ISA programs and their designs*

Over the last two decades, ISA programs have received increasing attention from both academics and practitioners. IS management has traditionally emphasized formalized rule structures against the background of a narrow technical

Table 1 – Consideration of design recommendations of ISA programs from literature.

Categories	Short description	References
Structure of ISA programs		
Media richness in ISA interventions	Refers to the utilization of diverse media material such as text or multimedia material, and the structure of the emergence of these materials. The richest medium is human telling the user about the IS issues.	(Abawajy, 2014; Shaw et al., 2009)
Customizing ISA interventions	Refers to customization of single components of an ISA program. Customization may apply to content, design and communication as well as to ISA interventions themselves. It is recommended to distinguish between cultures and countries.	(Ding et al., 2015; Karjalainen et al., 2013; Tsohou et al., 2015)
Implementation of an iterative control and improvement process	Refers to strategically planning and executing ISA programs by applying a staged and cyclic management process to ensure continuous quality improvements, such as the PDCA (Plan, Do, Check, Act) / Deming cycle.	(Disterer, 2013; Singh et al., 2013; Wilson and Hash, 2003)
Communication of ISA programs		
Non-technocratic IS risk and threat communication	Refers to IS managers' usage of a too technocratic language for ISA program interventions.	(Clarke et al., 2012; Peltier, 2005)
Message–person matching (personality)	Refers to the finding that users of a specific personality type are receptive to a specific kind of message or communication channel.	(Johnston et al., 2016; Kajzer et al., 2014)
Feedback interventions	Refer to a two-way communication enabled by IS managers which might be used to emotionally involve users through ISA program interventions.	(Eminağaoğlu et al., 2009)
Enforcement of reflection and dialogue	Refers to users' reflection of IS risks, either by a group or individually, which is reported to have a high impact on users' ISP compliance.	(Albrechtsen and Hovden, 2010)
Use of a role play (positive and negative)	Refers to users' identification with positive and negative characters in ISA programs. This identification might result in more emotional involvement.	(Karjalainen et al., 2013)

viewpoint to establish IS (Dhillon and Backhouse, 2001). In this view, prior research focused on formal controls implemented by policies, procedures or tools (Merete Hagen et al., 2008). From the late 1990s to the mid-2000s, work on ISA building and programs has increasingly utilized the socio-organizational perspective and was mainly conceptional in trying to understand how IS can be improved by increasing ISA. Initially, ISA programs were found to be deterrent countermeasures (Straub and Welke, 1998) and positioned to require a systematic planning approach (Puhakainen and Siponen, 2010; Siponen, 2000). In this stream prior research often applied the Deming cycle, e.g. relating to plan, do, check, act (PDCA) cycle models to visualize the continuous need of ISA building (Wilson and Hash, 2003). Users' achieved ISA is a temporal state of mind, which has to be renewed periodically (Warkentin et al., 2012; Wilson and Hash, 2003). Besides, IS risks are changing fast, and new technologies are challenging for users; hence, users have to be reminded often to stay aware (Clarke et al., 2012). Yet, organizations still seem to rely too much on formal methods, which are less resource demanding than ISA programs (Merete Hagen et al., 2008). Contemporary IS research asks for more balanced and holistic approaches (Tsohou et al., 2015).

While the importance of ISA for compliant IS behavior has now been clearly established (Bauer and Bernroider, 2015, 2017; Merete Hagen et al., 2008; Silic and Back, 2014; Siponen et al., 2014), there seems to be no commonly accepted agreement about how to effectively design ISA programs (Karjalainen et al., 2013). Prior literature offers several ISA program design recommendations and mixed results about the effectiveness of these approaches (Albrechtsen, 2007; Eminağaoğlu et al., 2009). Effectiveness refers to the ability of the ISA programs to increase individual ISA and improve users' ISP compliance. However, we assume that the contrary findings concerning ISA programs are likely due to the design diversity of the implemented ISA program in banks (Bauer et al., 2013; Shaw et al., 2009). Hence, we will proceed discussing recommendations for ISA programs focusing on the aspects of how ISA programs are structured and how stakeholders communicate ISA designs (see Table 1).

Previous studies take several perspectives to explain a lack of understanding on how ISA programs are communicated. Some studies identify language barriers that seem to play an important role among users (Albrechtsen and Hovden, 2009; Clarke et al., 2012; Peltier, 2005). Other recent studies identify specific personality types which diverge in their receptiveness of a specific kind of IS message and/or communication channel (Johnston et al., 2016; Kajzer et al., 2014) and recommend personality sensitive approaches to avoid ineffectiveness of initially proposed classic "one to many" mass communication (Kajzer et al., 2014). Literature on experiential learning approaches promote user involvement using several techniques to enforce a two-way communication on IS (Albrechtsen and Hovden, 2010; Clarke et al., 2012; Spears and Barki, 2010). For example, feedback interventions can be used to emotionally involve users and can lead to a two-way communication about IS (Eminağaoğlu et al., 2009). Building on learning theories, users' engagement can be enhanced by utilizing role models and role plays, which may lead to an increased users' identification with ISA programs and greater emotional involvement (Karjalainen et al., 2013).

Generally, studies that follow a diversified approach build on the main assumption that the way how users reflect on IS risks has an impact on their ISP compliance (Albrechtsen and Hovden, 2010). Overall, several ways can be employed to tackle ISA through communication aspects to finally improve users' compliant IS behavior.

Beyond the communication of ISA programs, there are also structural components that affect the effectiveness of their implementation. First, an iterative management cycle to ensure continuous improvements, such as the plan-do-check-act

(PDCA) cycle, is relevant (Disterer, 2013; Wilson and Hash, 2003). Such a model should in particular include a planning, an execution, an evaluation and an action stage on an ongoing iterative basis (Rantos et al., 2012). Further, media richness of the information channels is vital, because different kinds of learners perform better depending on media material such as text or multimedia material, and the structure of the emergence of these materials (Abawajy, 2014; Shaw et al., 2009). Last, but not least, customizing ISA interventions is recommended. One general template of an ISA program is unlikely to fit all divisions or units of an organization because of likely cultural differences in particular between countries and regions (Ding et al., 2015; Karjalainen et al., 2013).

2.2. *Employees' views on ISP compliance*

Despite the importance of an ISP for IS (Bauer and Bernroider, 2017; Lebek et al., 2014), users regularly neglect to act according to their organizational ISP (Siponen, 2000), and current research offers a range of different explanations (Albrechtsen, 2007; Albrechtsen and Hovden, 2009; Posey et al., 2014). The perception of IS risks plays a significant role for acting compliant with banks' ISP (Albrechtsen, 2007). IS manager tend to believe that unintentional ISP non-compliance of users is the greatest cause for IS incidents. In contrast, users regularly believe that external threats from hackers and the internet are the biggest IS risks, and do not see themselves as threats (Posey et al., 2014). Previous research highlights that most users do not understand and recognize significant IS risks, such as password misuse (Florencio and Herley, 2007; Horcher and Tejay, 2009). It is even less likely that users can estimate possible adverse impacts (Albrechtsen and Hovden, 2009; Posey et al., 2014). As a consequence, IS managers tend to blame users for not taking IS seriously enough and for generally underestimating the importance of IS for the organization (Albrechtsen and Hovden, 2009).

Another explanation for employee non-compliance is that people may lack the knowledge of the existence of the ISP and its content, which naturally is a pre-condition for ISP compliance (Wright, 2008). Previous research found that users' levels of ISP knowledge affect users' intentions to comply with ISP (Bauer and Bernroider, 2017; Pahnila et al., 2013). Unintentional violations of the ISP might result from users simply ignoring the existence of the ISP or users not caring or understanding the content of the ISP. Users and IS managers have different responsibilities concerning IS, which complicates managing ISP compliance. For users, who have to perform in their job mainly as a marketing assistant or bank counter employee, IS is most likely only a necessary secondary issue, which in turn may lead to justifying non-compliance, e.g., with work pressures (Barlow et al., 2013; Bauer and Bernroider, 2014). In principle, employees may use neutralization techniques to justify intentional ISP violations. Apart from time and work pressures, neutralization techniques can be related to perceived unjust rules, and the mentioned poor understanding of risks and possible threats (Siponen and Vance, 2010). The original theory was developed decades ago and focused on five techniques of neutralization (Sykes and Matza, 1957). Interestingly, Barlow et al. (2013) reported that certain techniques of neutralization are more powerful than others depending on the research context (e.g. defense of necessity for password security). In contrast, IS managers' primary role in their job is to ensure IS in the organization (Albrechtsen and Hovden, 2009, 2010) and work against these potential neutralizing behaviors. This study will explore tensions between groups of organizational members and implications for designing effective ISA programs.

3. Research methods

3.1. *Research approach*

We utilized a qualitative research design in three organizations in the banking sector utilizing different approaches to design and operate ISA programs. The organizations in the banking sector provided a relevant context for our research aims as those organizations are challenged by IS through internal and external pressures (e.g. Hsu et al., 2013; Goldstein et al., 2011).

In order to capture the phenomenon on IS within organizations we utilize a multiple case study design (Cavaye, 1996; Yin, 2014), utilizing data triangulation (Patton, 2002). Each organizational setting acts as a distinct bounded case. Furthermore, each organization is considered as an embedded case involving more than one unit of analysis (i.e. it relates to more than one branch and more than one individual user). We are particularly interested in a contrasting case study design (Eisenhardt, 1989; Stake, 2005) as it illuminates the distinct design approaches of ISA programs as well as diverse factors influencing ISP compliance in each organizational setting. In detail, each research case consists of interviews of bank branch as well as headquarters users, IS managers, and ISA program materials. This approach is suitable, as the interest of this study is not focused on one particular user but on how users' narratives reflect on ISP compliance and on design recommendations of ISA programs specifics. We develop propositions to enhance our understanding of ISP compliance and design recommendations for ISA programs (Eisenhardt, 1989).

3.2. *Data collection*

Our data collection followed three phases. First, informed by the literature review, we initiated a workshop in 2013 including focus groups to obtain a deeper understanding of IS and ISP compliance in the context of banking. This helped us to gain access to potential research partners within the organization. Second, we conducted 33 semi-structured interviews with IT professionals and users and analyzed ISA program materials such as intranet messages or leaflets (see stages exemplified in Fig. 1). The first stage of qualitative fieldwork was carried out from March to April 2013. We thereby gained deeper insights into the design and implementation of ISA programs. Building on those insights we conducted our semi-structured interviews with users of the three case banks from September 2013 to June 2014 (see Fig. 1 illustrates the research progress and stages).

Our sample comprises organizational members carrying out different roles, as indicated in Table A1. In total 33 interviews

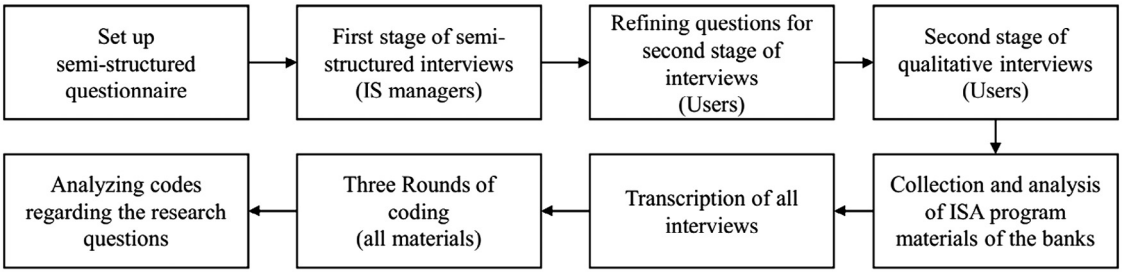

Fig. 1 – Research process.

were conducted with two groups of employees over two stages: 23 interviews with users, and 10 interviews with IS managers. As a result of our sampling strategy, interviewees were contacted according to their different roles they hold in the organizations (Myers and Newman, 2007), specifically we focused on two groups of employees: (1) IS managers: employees who design the ISA program. This includes IT security managers. Normally, they are not part of general management. (2) Users: employees, working in any business function, but not related to IS or IT. We recruited interview participants through several contacts within the respective banks, specifically through risk managers and their existing networks. Participants were contacted by email and assured of the research project's independence from the organization.

All interviews have been conducted in English, except the interviews in Gamma bank, which have been carried out in German. Each interview lasted between 30 and 40 minutes, was audio recorded with participants' prior consent, fully transcribed and anonymized (Sarker et al., 2013). Building on insights from our focus groups, during the first phase of investigation, we developed an interview guide including open-ended questions regarding information security in the respective bank. We started interviews by asking participants about their specific role in the bank, how they perceive information security risks within their bank, how they perceived the banks ISA programs.

3.3. *Data analysis*

In a first step, we explored narrative themes in our 33 interview transcripts. We read through the transcripts separately, aiming to capture the specific themes reviewing people's accounts as a "whole" while using N-Vivo to develop an initial coding structure. Building on these initial main categories, we continued to code across all interviews, developing main categories using content analysis (Huberman and Miles, 1994; Mayring, 2003). After coding, the researchers met again discussing the main categories and mutually validating the codes, internally and externally (Yin, 2014). Sequentially, our research strongly builds on an iterative process relying on data and conceptual insights from the literature for formulating propositions which reflects a deductive and inductive approach, integrating theoretical insights and emerging themes from our interview data.

4. Findings

Building on the following case descriptions, we discuss our main results in the subsections below. First, we start with an overview of the cases including the chosen ISA program approaches. Second, we present which ISA program designs are considered by the case banks. Third, employee groups and their problematic behaviors are described. Finally, factors influencing users' ISP compliance are analyzed in the three banks.

4.1. *Case overview*

The case study looked at three banks operating in Central Eastern Europe (CEE). All three institutions offer full-service including commercial banking (e.g. savings accounts and granting loans), investment banking (e.g. wealth and asset management) and other services (e.g. insurances). Since Basel II became effective, they set up units for operational risk to manage risks related to humans, processes, and information systems. Structurally, banks constituted IS departments responsible for ISA programs.

All three banks have some practices and established processes regarding IS in common. In terms of employee induction, for example, new employees have to complete a one-day training. The training includes compliance in particular related to IS and the knowledge required to comply with the respective ISP. Before users are allowed to begin their work and receive the necessary privileges, they have to sign an acknowledgment and acceptance of the ISP. All banks have also developed their own data classification by which they categorize their data based on its level of sensitivity and importance for the bank. Additionally, all banks have established different annual e-learning strategies addressing IS. However, the interviewed IS managers are not satisfied with the impact of e-learning on the users, who do not take the courses seriously enough, as, for example, this quotation demonstrates:

> People are speaking about the right answers, but only "which is right? B? Ok thanks", not about the topic. *IS Manager (B2), Beta bank.*

4.1.1. *Interaction approach (Alpha bank)*

After a phishing attack in 2006, Alpha bank started to plan their first ISA program and implemented it in 2007. The first ISA

program material dealt with the phishing attack and offered suggestions to users on how to deal with phishing attacks. The content was distributed via user newspapers and intranet. Since 2007, they conducted an ISA program annually and attempted to improve it from year to year. Alpha bank has developed ten IS policy documents focusing on different aspects of IS and has provided the ISPs on the intranet. In 2013, they conducted a campaign, which was structured in four weeks with changing themes every week and changing topics every day of the week, and with a quiz at the end of every week. This high interaction of users and IS managers fosters user involvement. The whole campaign is distributed in every branch. Furthermore, a role model, a fictitious employee, is used to deliver the content of the campaign. The role model character acts non-compliant, often communicating neutralizing behaviors to address common justifications of users. The IS managers collected opinions about the usefulness of their ISA program with a follow up questionnaire. More than 50% said that it was interesting and that they learned many new things.

4.1.2. *Incident-related approach (Beta bank)*

Beta bank began to conduct their ISA program in 2010. The main IS communication channel is the intranet, and it is used bi-weekly to deliver IS messages that are stored also in the intranet as articles. In these messages, the IS department tries to raise attention about actual risks gained from media, and they measure the diffusion of the messages by click rates. Hence, IS managers conclude that around 50% of all users at least view a new article. Last year, IS managers developed and implemented fake IS incidents to evaluate compliant behavior of their users in the headquarters and in branches. Beta bank is keen on communicating real incidents to the users, and hence their approach is named "incident-related". In addition to the focus on real incidents, Beta bank communicates the rules and working practices by emphasizing explanations to the users.

4.1.3. *Accountability approach (Gamma bank)*

Although Gamma bank set up their security department in 2009, they introduced their first ISA program by conducting monthly security tips in 2011. The security tips are frequently delivered through the intranet and saved. Moreover, every department of the bank has to have a yearly updated printed security folder, which addresses all necessary security topics, also including IS. Furthermore, IS managers evaluate compliant behavior with ISP of every branch and every business unit of Gamma bank once a year through short visits in which actual IS risks are simulated. Gamma bank set up a company agreement, which includes rights and obligations according to information technology and information handling, and every user must sign this company agreement. This proceeding enforces responsibility, which is additionally targeted by shifting security evaluation to line managers. Line managers have a short training on security topics, and once a year they have to fill out a "control sheet" in which they must report ISP compliance of users, such as clear desk policy or password. In addition, the line managers should evaluate access rights of the single users. Additionally, the bank maintains a blacklist with names of users who have conducted non-compliant behavior regarding ISP. IS managers contacted these users and explained their mistakes to them.

4.2. *Employee groups and IS behaviors*

Fig. 2 denotes three different internal employee groups considered in data analysis. We differentiated between two general user groups: headquarter and branch users. We realized that both groups face very different IS risks and behaviors. Headquarter employees are users working in the general management section of the banks (e.g. in marketing or project management). Branch employees are users facing and directly interacting with clients in branches. These distinctive profiles have strong implications for IS security behaviors, which should be influenced by ISA programs designed and run by IS managers.

> The risk is that the client manager wants to give the client the information fast, and the overcrowded daily routine sometimes… They think that security is just doing the wrong things. And it's hard to keep their mind about security. *IS manager (C7), Gamma bank.*

> Every policy rule cannot be carried out, every time, but I don't think the activities are so risky. *User (C8), Gamma bank.*

The analysis revealed that unintentional and intentional behaviors of users are likely to trigger IS incidents from the perspective of the users themselves as well as from IS managers overseeing their behaviors. Many users reported that co-workers have non-compliant password habits, have not implemented clear desk and screen policies, and follow undesirable information handling practices, as these responses show:

> Some colleagues do not care about a clear desk or clear screen. Everything lies everywhere, e.g. on the table. Documents such as balance sheets, customer information, nearly everything is unlocked on the table. *User (C9), Gamma bank.*

Furthermore, IS managers mention that the majority of users are aware of IS risks, but it seems that many intentionally act non-compliant with their ISP. According to IS managers, if only 2% of the users are not acting compliant with the ISP, then the entire bank is highly threatened.

> Yes, our employees are aware, but it's like risky driving on highway. They think "it can happen to everybody else but not to me". Hence, their behavior is not or not always in accordance with ISP. *IS manager (B1), Beta bank.*

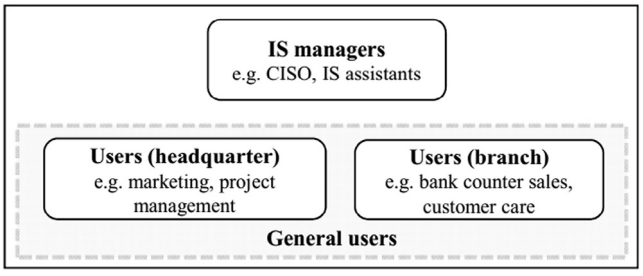

Fig. 2 – Overview of considered employee groups.

4.3. *Theme 1: ISA program designs*

The three banks have inconsistently implemented the design recommendations and can be classified into three different levels of coverage (see Table 2). In terms of structural design recommendations, only Alpha and Beta bank implemented the full PDCA cycle model, which consists of designing, developing, implementing, and monitoring an ISA program. In contrast, Gamma bank has not established an evaluation mechanism for ISA programs until now. Alpha bank does not only evaluate their ISA program, they also evaluate their users' behavior by conducting penetration tests, which include social engineering attacks. No bank has customized their ISA interventions for specific regions or branches. All banks have utilized media richness in their ISA programs.

Almost all communicational design recommendations have been considered by Alpha bank. In contrast, Beta and Gamma bank did not implement any of the recommendations. Specifically, several users of Beta and Gamma bank reported that the content of ISA program was too technocratic in many cases.

> I would say for me it [ISA program] is useful, but from time to time I receive some feedback that it is written too difficult, that it is written by lawyers, and not by speech of normal person (common tongue). *User (B3), Beta bank*.

In contrast, Alpha bank enforced reflection and dialogue because they query their users extensively with a questionnaire about how well they understood the interventions and how much they liked them after their ISA campaign.

> Sure the campaigns [ISA program] are a good method, because otherwise we [users] do not care so much about these kinds of things. Everybody will just do their job, and not care about information security issues. *User (A8), Alpha bank*.

Moreover, Alpha bank promoted active participation of their users by daily quizzes over one month and achieved a high number of participants in the quizzes. Beta and Gamma bank conducted no special measures to tackle users' involvement. Further, a role model, which enforces learning by imitation, has been included by Alpha bank to ensure users' involvement. Alpha bank also make use of social engineering penetration tests, which are defined as a feedback intervention, because they tackle users' behavior, and IS managers actively give feedback to the users about the adequacy of their behavior. The message-to-person matching recommendation with regard to users' personalities has not been considered in the considered ISA programs.

The majority of interviewees appreciated the implemented ISA program and perceived it as useful for their daily work. For example, Beta banks' users mentioned that it is valuable for them that real-life incidents are communicated via the ISA program. Nevertheless, some users are complaining about the interventions.

> I don't have a special place for it. It's only a cost benefit thing, so you can spend millions on something but still could have the risk of something happening. *User (B8), Beta bank*.

Some obstacles are found with intranet messages and e-mails as ISA interventions. Gamma banks' users often mentioned the high volume of messages arriving in the inbox in the morning. Current IS information is therefore often overlooked or receives a low priority compared to other emails. They also criticized the fact that IS information is sometimes presented in a complex and incomprehensible way, does not address the purpose, or is too abstract, as the following quotation shows.

> The security tips are a form of self-congratulation of the security department. They want that everybody is responsible. I do not like that practice. For example, today they wrote "Keep compliance with ISPs in mind". What should I do now? Look up the ISPs in the intranet and then pay attention? I do not believe that this is useful. It is only for the conscience of the IS managers. *User (C6), Gamma bank*.

Table 2 – Consideration of design recommendations of ISA programs in cases.

	Alpha bank	Beta bank	Gamma bank
Structural design recommendations			
Media richness of ISA interventions	Yes	Yes	Yes
Implementation of an iterative control and improvement process	Yes	Yes	No
Customizing ISA interventions	No	No	No
Communicational design recommendations			
Non-technocratic IS risk and threat communication	Yes	No	No
Message–person matching in regard to users' personalities	No	No	No
Enforcement of reflection and dialogue	Yes	No	No
Use of role models and role play	Yes	No	No
Feedback interventions	Yes	No	No
Overall coverage level of design recommendations	**High**	**Medium**	**Low**

4.4. *Theme 2: ISP compliance*

This theme includes the factors influencing ISP compliance among the banks.

4.4.1. *Perception of IS risks*

The users of Alpha bank seem to have a much higher level of IS risk perception in comparison with the two other banks. Alpha bank users more often connect IS with their daily routines, as the following statement of a product development manager show.

> An average risk is keeping the bank information secure. This secure information has to be defended and kept secure. The main problem for the bank is the data that the bank collects from the clients and stores in the secure server in this building or a secure data center. And the client needs this data for their company, and we have to send the clients

this data in a secure channel. This is the most difficult thing. The difficult part is the client wants to collect the data in a simple form, and the security for the client is not relevant in their daily routine. *User (A3), Alpha bank*.

Moreover, the investigation showed that different user groups reported different perceptions of IS risks. Interestingly, there are some differences between branch and headquarter users among all banks. For example, branch users seem to be generally aware of the risk of data leakage and also reported to be confronted with more and more social engineering attacks. In contrast, headquarter users see themselves to be not as important for ensuring IS. They mainly perceive IS risks from outside the bank (e.g. hackers) and do not regard their own behavior as very relevant for IS. It is important to note that also most headquarter users do not perceive their coworkers as potential malicious perpetrators.

4.4.2. *Perception of responsibilities, ISP importance, and knowledge*

The majority of users from all banks mentioned that everybody in the bank is responsible for IS. In contrast to this desirable statement, a few users and IS managers, especially from Beta and Gamma bank, mentioned that for some of their colleagues, IS does not really matter.

> It really depends on the attitude of staff members. The ones say: Yes that is necessary! The others say: No, leave me alone! *User (C4), Gamma bank*.

> There are sufficiently enough staff members who do not care. Honestly. *IS manager (C1), Gamma bank*.

> It is strange, because users tend to talk about problems at home with their PC, which was infected, etc. I think that they consider the electronic environment at work as secure, and take it for granted. They simply think that if we follow the rules, then it is secure, which is definitely a false feeling, because even the business environment can be somehow compromised or attacked or infected. *IS manager (B9), Beta bank*.

The reason for the lack of perveived responsibilities among a few users might be that the importance of IS in banks is not acknowledged by all users of Beta and Gamma bank. Users of both banks reported that they do not understand why security efforts, such as password security procedures, are important.

> Passwords are an infinite theme, I personally hate this issue. With our new rules for passwords, a minimum of 8 characters, Capital letters, numbers…. and you are not allowed to use the last 5 passwords. It is a very exhausting issue. And it doesn't matter if you log in on your computer or if you want to have access to the internet you always need your password. *User (C11), Gamma bank*.

Astoundingly, some IS managers of Beta bank seem to take also not every ISP for granted (e.g. secure internet use is seen to be not as important for ensuring IS). Further, the IS manager questions if technological safeguards are effective IS controls.

> I do not bother, as a security guy, if someone is watching naked girls or men on web pages in his office time, as long as he delivers his duty. That is a question for his manager to give him a proper measure of time. From my perspective, maybe those pages might be infected, but that is an annoyance, but not a real danger. If you try to block some of those pages, the only thing you do is you promote the creativity of the people to get there. They see it as a challenge, and that is the most dangerous thing you can encounter. *IS Manager (B9), Beta bank*.

Another explanation for the lack in perceived responsibilities could be missing knowledge about the content of the ISP. While the majority of users of all banks mentioned that they know the ISP, they often could not recall a single policy. Remarkably, most users know where to find the ISP and reported that they use the documents.

ISP enforcing activities, such as a compulsory signature of the ISP, is seen as an act of mistrust by many users. This was introduced in Gamma bank. The long-standing employees reported their disappointment and perceived mistrust when they had to sign the ISP and expected legal reasons to allow the bank to claim for compensation in case of an incident. Surprisingly, IS management also doubted this practice and critically scrutinized the benefits of this tactic.

4.4.3. *Use of neutralization techniques by users*

The respondents from Alpha bank indicated that their colleagues engage less in neutralization techniques when compared to the answers gained from Beta and Gamma banks. Many Beta and Gamma bank users seem to be justifying their non-compliant behavior with neutralization techniques and do not feel the same urgency to behave compliantly with the ISP. It seems that fulfilling their daily work tasks is prioritized over acting fully compliant. Surprisingly, there are differences between headquarter and branch users. Particularly branch users reported that their neutralizing behavior was due to a greater good, what can be categorized as the neutralization technique "Appeal to Higher Loyalties". Specifically, branch users struggle with heavy workload and in their daily business. Gamma bank's branch users highlight the customer focus, which complicates acting compliantly with ISP. The customer satisfaction focus requires the user to act quickly to answer inquiries, and users are often stressed because of the daily workload. This justification refers to the neutralization technique "defense of necessity", which implies that the user thinks he has no other acceptable choice.

> We stand with practically one leg in prison, because our customers would not understand why some things cannot be done for them. You always have to balance what you can say or do and what is not possible. *User (C11), Gamma bank*.

5. Discussion

ISA programs in banks can be viewed as complex preventive controls, which need to be designed and operationalized

carefully to overcome non-compliant IS behaviors of employees in relation to IS policies. We carefully analyzed cases of three different banks with different designs of ISA programs. First, our analysis was guided by different scopes of design recommendations identified in the literature. Second, we analyzed users' responses to capture technical and behavioral implications, which represent a diverse picture across banks and different user groups. In the following we discuss insights from our cases and present a set of interrelated research propositions summarizing our findings.

In terms of design recommendations, Alpha bank's ISA program design considered almost a full range of recommendations gained from literature and summarized in Tables 1 and 2. The interviews clearly indicated that this had a positive impact in terms lowering levels of perceived IS risks, acknowledging responsibilities, attributing importance to IS and building up knowledge of ISP, as well as mentioning neutralization techniques among colleagues to a lesser extent. In regard to the cases of Beta and Gamma bank, responses from users and IS managers indicate less comprehensive strategies were implemented and less positive implications were perceived. Based on our analysis, we conclude that a comprehensive design strategy seems to be more effective, which in terms of Alpha bank includes media richness (Shaw et al., 2009), an implementation of a full PDCA cycle (Wilson and Hash, 2003), non-technocratic IS risk communication (Clarke et al., 2012), feedback interventions (Eminağaoğlu et al., 2009), the use of role plays (Karjalainen et al., 2013), and enforcement of reflection and dialogue (Albrechtsen and Hovden, 2010). This observation leads us to our first proposition:

Proposition 1. The incorporation of a comprehensive mix of ISA interventions in ISA programs is likely to lead to improved levels of behavioral ISP compliance.

Regarding the structure of ISA programs, Alpha and Beta bank implemented a PDCA cycle model. The qualitative data showed that especially evaluation mechanisms are crucial for understanding the usefulness of ISA program interventions. Gaining this understanding on a timely basis seems to be essential for on-going improvements in terms of ISA program design choices and resulting ISA among employees. For example, some Gamma bank users mentioned that ISA interventions are seen as expressions of self-praise of the security department ("The security tips are a form of self-congratulation of the security department"). Therefore, without measuring the impact on users, the inefficacy of such self-congratulatory ISA interventions go unnoticed and will most likely fail to prevent IS incidents. Furthermore, respondents indicated that IS managers often lacked a long-term strategy in implementing their ISA programs, where such evaluation allows for revised planning. The strategies driving the ISA programs of Beta and Gamma bank were less characterized by prior planning and much more emergent in comparison with Alpha bank. The directions depended on current topics quickly selected on a quarterly basis and on the yearly approval of resources. Consequently, the single ISA interventions seemed isolated and were not well linked or coordinated in terms of a program. There was a lack of an explicit strategy taking into account a mix of approaches (following proposition 1) in which a risk and feedback based understanding guides the on-going selection of topics and methods in a management cycle. Our empirical findings support the views from prior research on the importance of feedback mechanisms (Eminağaoğlu et al., 2009) and the usefulness of incorporating such feedback in cycle models for managing ISA programs (Siponen, 2000; Straub and Welke, 1998; Wilson and Hash, 2003). The importance of a long-term strategy guiding the ISA program was barely covered by previous literature and extends previous findings. We therefore summarize as follows.

Proposition 2. The implementation of a long-term strategy allowing for the controlled adjustment of an ISA program based on careful evaluation is likely to lead to improved levels of behavioral ISP compliance.

Regarding how ISA programs are communicated, we identified Alpha bank's non-technocratic two-way communication solution as best practices example concerning their involvement of users. A dedication to non-technocratic IS risk communication was missing in the other two banks, where users reported that the ISP and also the IS interventions are not comprehensible enough. In particular, Gamma bank's ISA program interventions relied on formal and autocratic language ("I receive some feedback that it is written too difficult, that it is written by lawyers, and not by speech of normal person"). Our findings provide further empirical insights complementing the study of Clarke et al. (2012), which states that non-technocratic IS risk communication is crucial to create inclusiveness across user groups. Another successful approach to improve user involvement at Alpha bank included feedback interventions by conducting quizzes and role-plays. In addition, follow-up questionnaires were used as simple means to validate the usefulness of these ISA interventions. In contrast, Beta and Gamma bank did not implement any of these design recommendations. These results are consistent with the results of other current studies regarding the enforcement of reflection and dialogue (Albrechtsen and Hovden, 2010), use of role models and role plays (Karjalainen et al., 2013), and feedback interventions (Eminağaoğlu et al., 2009) to positively influence ISA. Accordingly, we raise another proposition.

Proposition 3. Non-technocratic two-way communication in an ISA program is likely to lead to improved levels of behavioral ISP compliance.

Banks generally neglected to customize their ISA interventions (Karjalainen et al., 2013) to regional contexts, organizational entities, and or tailor interventions to IS risks more common among certain employee groups, and did not consider personality profiles (Johnston et al., 2016; Kajzer et al., 2014). However, both aspects related with differentiated IS interventions seem to be important for the investigated banks. The location of the branch was reported to be connected with different IS requirements. IS managers mentioned that the location of the brand can determine the likelihood or severity of IS risks. Beta bank, for example, has a southern region more prone to phishing attacks, while password misuse is more likely in their country's capital. The physical separation with users distributed in several hundred branches is one main barrier.

Another issue is that collecting data on user's personality traits would require large time investments and approval from employee representatives. Accordingly, while interviewed IS managers found differentiation promising, they also mentioned that it is difficult to implement.

Our empirical analysis emphasized the salience of two large groups of users in banks, which face different IS risks and have different needs of information in their work areas (headquarter vs. branch user). For example, branch users struggle more with safely logging on and off from the computers ("Passwords are an infinite theme, I personally hate this issue"), while this is not an issue for headquarter users. Hence, we suggest that there should be a clear differentiation between these groups of employees in ISA programs (and possibly others) according to their needs, despite the fact that the rules of ISP are binding for all. Our research extends current literature (Albrechtsen and Hovden, 2009; Posey et al., 2014) by calling for a more differentiated target audience concept and, hence, we raise the following proposition.

Proposition 4. The differentiation of target audiences (e.g. headquarter and branch users) in ISA programs is likely to lead to more effective ISA interventions and consequently to improved levels of behavioral ISP compliance.

While the level of knowledge of the ISP is consistently low among users in all banks, we found that users of Alpha bank (with a high coverage level of design recommendations) have different perceptions about their responsibilities and duties regarding ISP compliance. Headquarter and branch users are not recognizing their own responsibilities in ensuring IS and instead assign responsibility to IT/IS personnel. This finding extends existing IS research by providing insights into perceived IS responsibilities, which seems to differ between employee groups (Albrechtsen, 2007; Albrechtsen and Hovden, 2009; Kolkowska, 2011; Posey et al., 2014).

Intentional violations of the banks' ISP are usually justified by users among our cases in the form of neutralization techniques. While ISA programs can reduce the use of neutralization techniques and enhance the likelihood that those users will follow the banks' ISP, no case focused on communicating ISA interventions based on the prevention of neutralization techniques (Barlow et al., 2013; Bauer and Bernroider, 2014). Branch users are reverting mostly to "appeal to higher loyalties" and "defense of necessity" ("We stand with practically one leg in prison, because our customers would not understand why some things cannot be done for them"). Both, branch and headquarter users commonly utilize the technique "denial of injury". This differentiation adds to previous qualitative research on ISA (Albrechtsen, 2007; Albrechtsen and Hovden, 2009; Posey et al., 2014). Additionally, we provide new insights to existing research on neutralization and IS policy compliance (Barlow et al., 2013; Bauer and Bernroider, 2017; Siponen and Vance, 2010). According to the above differentiation proposition, we extend it by assuming that ISA interventions, which specifically target particular neutralization techniques of headquarter or branch users, should more effectively tackle neutralizing behaviors. Thus, we raise the following final proposition.

Proposition 5. ISA programs considering user group tailored interventions are more likely to reduce the particular neutralization techniques common to the according user group.

Finally, we also distinguished between different types of ISA programs based on dominant characteristics and classified three different approaches: Alpha Bank implementing an interaction approach, Beta Bank an incident approach, and Gamma bank an accountability approach. The interaction approach focuses on user involvement helped IS managers to get feedback about their ISA interventions and employees' perceptions of actual IS risks. Beta bank's incident approach allowed users to better conceive actual IS risks in contrast to Gamma bank's users, who report that they missed examples of real-world IS incidents. While the Gamma bank's accountability approach has the advantage that users feel more responsible than in other banks, the chosen ISA interventions also induced a feeling among users of being mistrusted. Overall, every approach has specific benefits, which could be potentially combined in a mixed-form approach.

5.1. *Implications for practice*

Based on our findings, the following implications for practice offer suggestions for the design of effective ISA programs, which may also provide value to organizations from other industries apart from financial services. We also give illustrative examples to specifically demonstrate how IS managers could improve their ISA programs based on the above discussed propositions.

In relation to proposition 1, we suggested that IS managers should implement a mix of ISA design recommendations outlined in Table 1 and control whether users are getting involved and find ISA program useful. This mix of ISA interventions could, e.g., in terms of media richness include innovative ISA videos visualizing IS risks and threats, which can be today produced relatively economically or may even be developed by users (Bauer and Frysak, 2014). In such ways, employees not consuming the information via other more traditional channels such as emails can be reached. Another example would be to scare users by illustrating real life stories of IS incidents in ISA programs without applying a technocratic style. For example, IS management is advised to avoid advocating purely technical knowledge detailing rules for hard passwords from the top (Horcher and Tejay, 2009). We noted that IS managers, utilizing an incident approach based on simple and engaging stories about real life IS incidents, achieved greater user involvement. Users may even be encouraged to share their own experiences and what they have learned from mistakes. A good example is to expose bad password use and reuse habits and possible adverse impacts (Florencio and Herley, 2007), which may be published in an ISA video, a blog post or an intranet podcast.

In terms of proposition 2, we in particular point to the lack of an evaluation mechanism in IS management preventing improvements of ISA programs. IS managers should introduce a full cycle model, which should be iteratively applied such as the commonly known PDCA cycle (Disterer, 2013; Wilson and Hash, 2003). Our findings emphasize the importance of evaluation and careful study of ISA interventions, which should be

aligned with the needs of different user groups in aiming at the prevention and detection of changing IS risks and threats. The impact of ISA programs on ISA and possibly the resulting users' security behavior should be measured with suitable metrics to allow for managing the effects of each ISA intervention on the different user audiences of the organization. While there is no prescriptive set of metrics which can be generally prescribed, supporting standards or frameworks, e.g. COBIT or ISO2700X (Sahibudin et al., 2008), can be used to guide the selection of IS metrics. The type and focus of the intervention will determine the aspect of ISA to measure. For example, if access control habits are targeted, password cracking software or sampling walk-throughs where, e.g., unattended screens without password protection are sought, can be used to measure levels of compliant IS behaviors (Peltier et al., 2005). A new trend is the use of honeypots to foster the understanding about how compliant or fraudulent users behave (Christopher et al., 2017). Among banks, the costs and frequency of all IS incidents are usually measured by their operational risk departments, which can be used to indirectly estimate the effectiveness of the ISA program. Some banks evaluate IS policy compliance directly by, e.g., applying social engineering penetration tests (Bullée et al., 2015). Usually, penetration tests are conducted by external agencies, which actively check users' behavior in terms of handling fake phishing mails, fake phone calls and fake artifacts such as USB sticks, which users should not connect with their computers (Bauer et al., 2013). The findings from Alpha bank, however, showed that such assessment practices can be disturbing for users, because they feel overly controlled by their employer. Alternatively, measurements could involve self- or peer-assessments, either qualitatively or quantitatively (Vaughn et al., 2003).

In the context of proposition 3, feedback interventions can be built into ISA programs to enable effective two-way communication. For example, the above mentioned self-assessments would also support user involvement and allow for feedback in an ISA program. The feedback can also be fostered by engaging in dialogs with users (e.g. by utilizing role-plays or quizzes). In our case study, Alpha bank utilized creative approaches to enhance user's emotional involvement in this way. The use of role models stimulated discussions in rather informal settings, e.g., during lunch time, to lower the barriers for reflecting on information distributed earlier. This setting fostered ISA relevant discussions among users, which then also became more willing to conduct the quizzes. It is suggested to design questions around main themes previously emphasized in other ISA program interventions to support repetitive learning and build on prior knowledge, which is also likely to reinforce shared knowledge and group learning (David et al., 2016). Another example to foster two-communication is the use of common language and user friendly non-technocratic vocabulary in ISA program interventions. Our third case, Gamma bank, revealed a set of pitfalls by showing how banks should not communicate in this context, e.g., the dissemination of directive messages highlighting that employees must stay compliant to the ISP. This approach created irritations and misunderstandings about the content of ISP and resulted in largely detached users.

Propositions 4 and 5 suggest differentiated approaches in ISA programs designs. First of all, IS management could customize ISA programs by user groups (e.g. headquarter vs. branch users) and by geographical areas, which are likely to have cultural differences relevant for internalizing ISA (Tsohou et al., 2015). Similar to target marketing approaches, IS managers should first evaluate the needs and characteristics of single user groups regarding ISP compliance. Next, they should customize ISA interventions to more effectively address certain groups of users. The headquarter/branch structure has some particular implications for ISA programs such the need for covering widely distributed units. Interventions can also be tailored to reduce particular neutralization techniques identified as highly relevant in our context of ISP compliance in banks. Practitioners should consider tackling the neutralization techniques denial of injury, appeal to higher loyalties, and defense of necessity in their ISA programs. To mitigate the latter, e.g., user perceptions of IS responsibilities can be targeted to balance IS and operational pressures, which users face when conducting their daily tasks.

5.2. *Implications for future research*

Our findings offer many possibilities for future research in the area of ISA program designs. Research has only begun to identify recommendations for effective structural or communicational designs. Particularly the involvement of users seems to have an important mediation effect, and research could explore in more detail how involvement is reached through ISA interventions, which should in turn foster behavioral ISP compliance. We offer a list of propositions, which could be used to inform model development and be tested in a quantitative survey. Further, message-to-person congruence in ISA interventions was not analyzed through the underlying study because to our best of knowledge no case considered this factor so far. Therefore, future research should analyze which types of personalities are more sensitive to certain ISA interventions or ISA program approaches in practice. In terms of structure, further research is necessary to discover different ISA program approaches. This study only identified ISA programs with three different foci, and further research on the relationship or investigating a mix of different types of ISA interventions is still needed.

Users' ISP compliance still needs to be explored empirically in more depth in banks and other industries. In particular, more qualitative research might focus on certain user perspectives. It can be expected that other industries face similar problems as banks in enforcing ISP compliance, and the differentiation between headquarter and branch users (or other groups) offers an interesting area for research. Regarding the individual level, future studies on intentional violations of banks' ISP could expand on the three neutralization techniques: denial of injury, appeal to higher loyalties, and defense of necessity. Our results showed that these are highly important in the context of banks.

The short-, mid-, and long-term effect of ISA programs on users' ISP compliance could be analyzed with longitudinal quantitative research. As we described, users' achieved ISA is a temporal state of mind, but ISA programs with several ISA interventions over time should work toward maintaining a high level of ISA throughout the workforce. Therefore, a longitudinal study could more accurately identify effects of ISA programs on users' ISP compliance.

5.3. *Limitations*

Several limitations have to be considered concerning our results and interpretations. First, we have researched three banks in the CEE region. Therefore, the data represents very specific cases and allows unique insights into usually tightly sealed IS contexts, which however cannot be generalized. Second, talking about security issues within the respective workplace could be biased by social desirability and other factors. We tried to overcome respondents' social desirability answering behavior by asking users if coworkers neutralize their ISP violations and thereby not directly asked about their own behavior. Third, the case study is also bounded to the context, situations, and time. Generally, narratives offer a rich material from retrospective construction of stories to illustrate insights relevant for the case.

6. Conclusion

The multiple case studies revealed that different coverage levels of ISA program design recommendations are likely to influence a wide area of factors related to users' ISP compliance. This calls for further research on ISA program designs as well as on the identified factors influencing ISP compliance. Structural as well as communicational design recommendations are critical for the enforcement of two-way communication, for which especially the use of feedback interventions is advantageous. Overall, we recommend that IS managers should pay more attention to a cyclic management process, such as the PDCA cycle, to in particular incorporate ISA program evaluation and adaptations. A high coverage level of suggested design recommendations is likely to improve perceptions of IS risk, responsibilities, ISP importance, and knowledge as well as a lesser use of neutralization techniques. In detail, the best practice case of Alpha bank showed that their interactive approach seems to be most beneficial for increasing IS risk perceptions. Additionally, in designing ISA programs, IS managers should consider a more differentiated concept to effectively reach all users. Banks as well as other information centric organizations should customize their ISA programs by distinguishing between the IS needs of user groups, in terms of headquarter and branch users.

Appendix

Table A1 – Interview statistics (all interviews face-to-face, average duration 33 minutes).

ID	Role description	Case	Role	Interview code
1	Head of information security department	Alpha bank	IS managers	A1
2	Retail risk manager	Alpha bank	User	A2
3	Product development manager	Alpha bank	User	A3
4	Marketing manager	Alpha bank	User	A4
5	Secretary	Alpha bank	User	A5
6	Corporate risk management analyst	Alpha bank	User	A6
7	Branch advisor	Alpha bank	User	A7
8	Head of control systems	Alpha bank	User	A8
9	Law operations manager	Alpha bank	User	A9
10	Head of information security	Beta bank	IS managers	B1
11	Head of information security	Beta bank	IS managers	B2
12	Communication manager	Beta bank	User	B3
13	Audit manager	Beta bank	User	B4
14	General manager direct banking	Beta bank	User	B5
15	Operational risk manager	Beta bank	IS managers	B6
16	Business continuity manager	Beta bank	User	B7
17	Non-cash transactions manager	Beta bank	User	B8
18	Physical security manager	Beta bank	IS managers	B9
19	Fraud prevention analyst	Beta bank	IS managers	B10
20	Project manager	Beta bank	User	B11
21	Assistant to chief security officer	Gamma bank	IS managers	C1
22	Education and training coach	Gamma bank	IS managers	C2
23	IT security manager	Gamma bank	IS managers	C3
24	Accounting employee	Gamma bank	User	C4
25	Branch manager	Gamma bank	User	C5
26	Branch manager	Gamma bank	User	C6
27	IT security and organization	Gamma bank	IS managers	C7
28	Branch manager	Gamma bank	User	C8
29	Advisor for corporate clients	Gamma bank	User	C9
30	Client advisor	Gamma bank	User	C10
31	Lawyer and system manager	Gamma bank	User	C11
32	Client advisor	Gamma bank	User	C12
33	Assistant to the executive board	Gamma bank	User	C13

Table A2 – Coding scheme.

Codes: main-themes	Short description	Total instances
ISA program		
ISA program	Statements and verbal evidence of IS managers about the ISA programs of the banks.	148
Organization and structure of ISA program	How the IS managers plan, organize and structure their ISA programs.	60
Organizational integration of IS management	Statements about the organization of IS and how organizational units work together to ensure IS.	21
Perception of usefulness of ISA program	Users' perception of the usefulness and effectiveness of ISA program for ensuring IS in the banks.	46
Perception of usefulness of ISA interventions	Users' perception of the usefulness and effectiveness of single ISA interventions for ensuring IS in the banks.	37
Factors influencing ISP compliance		
Perceived IS risks	The IS risks that users perceive in their bank. The code includes also the description of the risks and threats.	155
Perceived knowledge of ISP	Statements and verbal evidence for users' knowledge of the content of IS policies.	15
Perceived importance of ISP	Users' perception of importance of ISP compliance.	22
Perceived responsibilities regarding ISP	Users' perception of responsibilities of ISP regarding ISP.	27
Use of neutralization techniques	Neutralization techniques are cognitive justifications to excuse users' undesirable information security behavior.	25

REFERENCES

Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):237–48.

Albrechtsen E. A qualitative study of users' view on information security. Comput Secur 2007;26(4):276–89.

Albrechtsen E, Hovden J. The information security digital divide between information security managers and users. Comput Secur 2009;28(6):476–90.

Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Comput Secur 2010;29(4):432–45.

Barlow JB, Warkentin M, Ormond D, Dennis AR. Don't make excuses! Discouraging neutralization to reduce IT policy violation. Comput Secur 2013;39:145–59.

Baskerville R, Spagnoletti P, Kim J. Incident-centered information security: managing a strategic balance between prevention and response. Inf Manag 2014;51(1):138–51.

Bauer S. 2012. A literature review on operational it risks and regulations of institutions in the financial service sector. Paper presented at The International Conference of Information Resources Management (Conf-IRM).

Bauer S, Bernroider EWN. 2014. An analysis of the combined influences of neutralization and planned behavior on desirable information security behavior. Paper presented at the 13th Annual Security Conference, Las Vegas, US.

Bauer S, Bernroider EWN. 2015. The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring. Lecture Notes in Computer Science (LNCS), Vo. Human Aspects of Information Security, Privacy, and Trust (LNCS 9190), 154–164.

Bauer S, Bernroider EWN. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. The Data Base Adv Inf Syst 2017;48(3):1–24.

Bauer S, Frysak J. Developing a viral artifact to improve employees' security behavior. Int J Soc Behav Educ Econ Bus Indus Eng 2014;8(8):2449–52.

Bauer S, Bernroider EWN, Chudzikowski K. 2013. End user information security awareness programs for improving information security in banking organizations: preliminary results from an exploratory study. Paper presented at the AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013), Milano.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34(3):523–48.

Bullée J-WH, Monotoya L, Pieters W, Junger M, Hartel PH. The persuasion and security awareness experiment: reducing the success of social engineering attacks. J Exp Criminol 2015;11(1):97–115.

Cavaye ALM. Case study research: a multi-faceted research approach for IS. Inf Syst J 1996;6(3):227–42.

Christopher L, Choo K-KR, Dehghantanha A. Honeypots for employee information security awareness and education training: a conceptual EASY training model. In: Choo K-KR, Dehghantanha A, editors. Contemporary digital forensic investigations of cloud and mobile applications. Cambridge: Elsevier; 2017. p. 110–28.

Clarke N, Stewart G, Lacey D. Death by a thousand facts. Inform Manag Comput Secur 2012;20(1):29–38.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32:90–101.

David JY, Shin HC, Pérez I, Anderies JM, Janssen MA. Learning for resilience-based management: generating hypotheses from a behavioral study. Glob Environ Change 2016;37:69–78.

Davidson J. 2016. FDIC reports five "major incidents" of cybersecurity breaches since fall. The Washington Post.

Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Inf Syst J 2001;11(2):127–53.

Ding Y, Meso P, Xu S. 2015. A theoretical model for customizable learning/training to enhance individuals' systems security behavior. Paper presented at the 21st Americas Conference on Information Systems (AMCIS), Puerto Rico, USA.

Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management. J Inf Secur 2013;4(2):92–100.

Eisenhardt KM. Building theories from case study research. Acad Manage Rev 1989;14(4):532–50.

Eminağaoğlu M, Uçar E, Eren Ş. The positive outcomes of information security awareness training in companies – a case study. Inf Secur Tech Rep 2009;14(4):223–9.

EU. Directive 2006/43/EC. Official J Eur Union 2006;147(87):1–21.

EU. Directive 2009/138/EC. Official J Eur Union 2009;335(2):1–155.

Florencio D, Herley C. 2007. A large-scale study of web password habits. Paper presented at the Proceedings of the 16th international conference on World Wide Web.
Gillet R, Hübner G, Plunus S. Operational risk and reputation in the financial industry. J Bank Financ 2010;34(1):224–35.
Goel S, Shawky HA. Estimating the market impact of security breach announcements on firm values. Inf Manag 2009;46(7):404–10.
Goldstein J, Chernobai A, Benaroch M. An event study analysis of the economic impact of IT operational risk and its subcategories. J Assoc Inf Syst 2011;12(9):606–31.
Goodhue DL, Straub DW. Security concerns of system users: a study of perceptions of the adequacy of security. Inf Manag 1991;20(1):13–22.
Guo KH. Security-related behavior in using information systems in the workplace: a review and synthesis. Comput Secur 2013;32:242–51.
Horcher A-M, Tejay GP. 2009. Building a better password: The role of cognitive load in information security training. Paper presented at the IEEE International Conference on Intelligence and Security Informatics.
Höne K, Eloff JHP. Information security policy – what do international information security standards say? Comput Secur 2002;21(5):402–9.
Hsu C, Backhouse J, Silva L. Institutionalizing operational risk management: an empirical study. J Inf Tech 2013;29(1):59–72.
Huberman AM, Miles MB. Data management and analysis methods. Thousand Oaks, CA: Sage Publications, Inc; 1994.
Jobst AA. It's all in the data – consistent operational risk measurement and regulation. J Financ Regul Compliance 2007;15(4):423–49.
Johnson EC. Security awareness: switch to a better programme. Netw Secur 2006;2006(2):15–18.
Johnston AC, Warkentin M, McBride M, Carter L. Dispositional and situational factors: influences on information security policy violations. Eur J Inf Syst 2016;25(3):231–51.
Kajzer M, D'Arcy J, Crowell CR, Striegel A, Van Bruggen D. An exploratory investigation of message-person congruence in information security awareness campaigns. Comput Secur 2014;43:64–76.
Karjalainen M, Siponen M, Puhakainen P, Sarker S. 2013. One size does not fit all: different cultures require different information systems security interventions. Paper presented at the The Pacific Asia Conference on Information Systems (PACIS).
Kjaerland M. 2005. A differentiation between reported computer security incidents directed towards the bank/finance sector. In: Bilsky and D. Elizur, (Eds.), *Facet Theory: Design, Analysis & Applications*, 221–231.
Kolkowska E. 2011. Security subcultures in an organization – exploring value conflicts. Paper presented at the The 19th European Conference on Information systems (ECIS), Helsinki.
Lebek B, Uffen J, Neumann M, Hohler B, Breitner MH. Information security awareness and behavior: a theory-based literature review. Manag Res Rev 2014;37(12):1049–92.
Luthy D, Forcht K. Laws and regulations affecting information management and frameworks for assessing compliance. Inform Manag Comput Secur 2006;14(2):155–66.
Mayring P. Qualitative Inhaltsanalyse: Grundlagen und Techniken. 8th ed. Weinheim: Beltz; 2003.
Merete Hagen J, Albrechtsen E, Hovden J. Implementation and effectiveness of organizational information security measures. Inform Manag Comput Secur 2008;16(4):377–97.
Myers MD, Newman M. The qualitative interview in IS research: examining the craft. Inf Org 2007;17(1):2–26.
Norton J, Walker G. Banks: fraud and crime. CRC Press; 2014.
ORX, Report on Operational Risk Loss Data, Operational Riskdata eXchange Association (ORX); 2014. Available from https://managingrisktogether.orx.org/. [Accessed 12 December 2015].
Pahnila S, Karjalainen M, Siponen M. 2013. Information security behavior: towards multi-stage models. Paper presented at the Pacific Asia Conference on Information Systems (PACIS), Jeju Island (Korea).
Patton MQ. Qualitative interviewing. Qual Res Eval Methods 2002;3:344–7.
Peltier TR. Implementing an information security awareness program. Inf Syst Se 2005;14(2):37–49.
Peltier TR, Peltier J, Blackley JA. Information security fundamentals. Florida, US: CRC Press; 2005.
Posey C, Roberts TL, Lowry PB, Hightower RT. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Inf Manag 2014;51(5):551–67.
PricewaterhouseCoopers. 2014. Information security breaches survey. The Department for Business, Innovation and Skills, BIS/14/767.
Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. MIS Q 2010;34(4):757–78.
Rantos K, Fysarakis K, Manifavas C. How effective is your security awareness program? An evaluation methodology. Inf Secur J 2012;21(6):328–45.
Sahibudin S, Sharifi M, Ayat M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. Paper presented at the Second Asia International Conference on Modeling & Simulation.
Sarker S, Xiao X, Beaulieu T. Qualitative studies in information systems: a critical review and some guiding principles. MIS Q 2013;37(4):iii–xviii.
Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Comput Educ 2009;52(1):92–100.
Shukla S, Bhakta P. 2016. 3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit. The Economic Times.
Silic M, Back A. Information security: critical review and future directions for research. Inform Manag Comput Secur 2014;22(3):279–308.
Singh AN, Picot A, Kranz J, Gupta MP, Ojha A. Information Security Management (ISM) practices: lessons from select cases from India and Germany. Glob J Flex Syst Manag 2013;14(4):225–39.
Siponen M. A conceptual foundation for organizational information security awareness. Inform Manag Comput Secur 2000;8(1):31–41.
Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q 2010;34(3):487–502.
Siponen M, Mahmood MA, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manag 2014;51(2):217–24.
Spears JL, Barki H. User participation in information systems security risk management. MIS Q 2010;34(3):503–22.
Stake RE. Qualitative case studies. In: Denzin NK, Lincoln YS, editors. The Sage handbook of qualitative research. 3rd ed. Thousand Oaks, CA: Sage; 2005. p. 443–66.
Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Comput Secur 2005;24(2):124–33.
Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Q 1998;22(4):441–69.

Sykes GM, Matza D. Techniques of neutralization: a theory of delinquency. Am Sociol Assoc 1957;22(6):664–70.
Thomson ME, von Solms R. Information security awareness: educating the users effectively. Inform Manag Comput Secur 1998;6(4):167–73.
Tsohou A, Karyda M, Kokolakis S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput Secur 2015;52:128–41.
US-Congress. 2002. Sarbanes-Oxley Act of 2002 (pp. 66). Washington: One Hundred Seventh Congress of the United States of America.
Vaughn RB, Henning R, Siraj A. 2003. Information assurance measures and metrics-state of practice and proposed taxonomy. Paper presented at the 36th Annual Hawaii International Conference on System Sciences.
Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. Eur J Inf Syst 2009;18(2):101–5.
Warkentin M, Straub D, Malimage K. 2012. Featured talk: measuring secure behavior: a research commentary. Paper presented at the Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY.
Wilson M, Hash J. Bement AL, editor. Building an information technology security awareness and training program. Gaithersburg: National Institute of Standards and Technology (NIST) Special Publication; 2003. p. 800–50.
Wright CS. Assessing security awareness and knowledge of policy. In: The IT regulatory and standards compliance handbook: how to survive information systems audit and assessments. Syngress; 2008. p. 161–94.
Yin RK. Case study research: design and methods. 5th ed. Thousand Oaks: Sage Publications, Inc; 2014.

Stefan Bauer is a digital strategist in an Austrian bank and a lecturer at University of Applied Sciences Technikum Wien. In 2016 he received a doctoral degree in Information Systems from the Vienna University of Economics and Business. Among others, his research interests include management of information security, corporate accelerators and digital innovation. He currently engages in a project researching digital transformation of the banking industry.

Katharina Chudzikowski is Associate Professor in Organisation Studies at the School of Management, University of Bath. She is interested in understanding work situated in different settings. Her current interest focuses on how professionals are embedded in organizations and how this influences perceptions and ways of organizing in knowledge intensive contexts.

Edward Bernroider is Professor of Management Information Systems and Head of the Department of Information Systems and Operations at WU Vienna (Vienna University of Economics and Business) in Austria. His current interests reflect a concern for assessing and developing IS capabilities and how these can positively impact individuals, organizations and entire societies. He has engaged in a variety of educational programs, international consultancies, and advisory activities for commercial and nonprofit enterprises, and made numerous presentations at national and international conferences. His publications have appeared in top rated journals such as the Journal of Information Technology, European Journal of Information Systems, Decision Support Systems, Information & Management, European Journal of Operational Research, Computers & OR, and the Business Process Management Journal.