The Role of Information Security Awareness for Promoting Information Security Policy Compliance in Banks

Bauer, Stefan

DOI:
10.57938/1de330f8-daa1-42d9-9457-1b9e0249db6b

Published: 14/03/2016

Document Version
Unknown

DOKTORAT DER SOZIAL- UND WIRTSCHAFTSWISSENSCHAFTEN

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

1. Beurteilerin/1. Beurteiler: **Univ.Prof. Dr. Edward W. N. Bernroider**

2. Beurteilerin/2. Beurteiler: **ao.Univ.Prof.Dr. Alexander Kaiser**

Eingereicht am: _____

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

Titel der Dissertation:

The Role of Information Security Awareness for Promoting Information Security Policy Compliance in Banks

Dissertation zur Erlangung des akademischen Grades

einer Doktorin / eines Doktors

der Sozial- und Wirtschaftswissenschaften an der Wirtschaftsuniversität Wien

eingereicht bei

1. Beurteilerin/1. Beurteiler: **Univ.Prof. Dr. Edward W. N. Bernroider**

2. Beurteilerin/2. Beurteiler: **ao.Univ.Prof.Dr. Alexander Kaiser**

von **Stefan Bauer**

Fachgebiet: **Wirtschaftsinformatik**

Wien, im **März 2016**

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

Ich versichere:

1. dass ich die Dissertation selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

2. dass ich diese Dissertation bisher weder im In- noch im Ausland (einer Beurteilerin/ einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

3. dass dieses Exemplar mit der beurteilten Arbeit übereinstimmt.

Datum _____ Unterschrift _____

The Role of Information Security Awareness for Promoting Information Security Policy Compliance in Banks

Dissertation

to obtain the academic degree of a

Doctor rerum socialium oeconomicarumque

(Dr.rer.soc.oec.)

submitted to the Vienna University of Economics and Business

Department of Information Systems and Operations

Institute for Information Management and Control

by

Stefan Bauer

Vienna, March 2016

Supervisor: Prof. Edward W.N. Bernroider
Second Supervisor: Prof. Alexander Kaiser

Submitted by: Stefan Bauer
Hauptstraße 97
2171 Herrnbaumgarten
+436769088083
Stefan.Bauer@wu.ac.at

Contents

Acknowledgments

"It is good to have an end to journey toward; but it is the journey that matters, in the end."
(Ernest Hemingway)

Through this journey, I have met many people, who I would like to thank for their advices and kindness. First, it is important to me to express my great thankfulness to my supervisor, Prof. Edward Bernroider, who supported, helped, and advised me through the entire journey of this dissertation. Thank you very much for all your time and efforts. Further, I would like to give my sincere thanks to Katharina Chuzikowski, who supported and helped me in the qualitative research stages. Next, I like to thank the team of the Institute of Information Management and Control, namely Eversit Limaj, Josef Frysak, Sebastian Margiol, Petra Pajic, Roman Brandtweiner, and Barbara Krumay, for their assistance and great moral support. Moreover, I want to thank my former colleagues, Nikolaus Obwegeser and Konradin Maier, for their support in the first years of my dissertation. Special thanks also to my former colleague Alexander Novotny, who has always had an open ear for countless discussions about our research topics. Finally, yet importantly, I want to thank the other supervisors of this thesis, Prof. Roman Brandtweiner, Prof. Alexander Kaiser, and Prof. Bernd Simon, for their time and efforts in recent years.

Second, I take this opportunity to thank my parents, Karl and Margit, for making my university studies possible. Thank you for giving me the opportunity to study in difficult times, which enabled my personal development and allowed me to find my own path. Additionally, I would like to highlight the helping hand of my sister, Daniela, when I was having difficulties in school as well as in my studies. Without my parents and my sister, I may never have gotten to where I am today. Further, I want to thank my girlfriend, Martina, for her advice and the patience with which she endured all the ups and downs of the dissertation process. In addition, I want to thank all the members of my family for their help.

Finally, I would like to acknowledge all my friends for their moral support over the last years. Special thanks to my close friends, Jim Brito, Maximilian Höltl, Alexander Lopez, and Marko Frankovic, who all encouraged me to go the extra mile for success over the last ten years. Also, special thanks to my very old and close friends, Josef Ebenauer, Christoph Schodl, and Peter Burger, for giving support in difficult times.

Abstract

Banks rely heavily on information security (IS) by preserving confidentiality, integrity, and availability of information. A key layer for ensuring information security is the employees, who need to be aware of possible information security issues and behave accordingly. Banks introduce information security policies (ISP) to establish required rules for IS behavior and implement information security awareness (ISA) programs, which are systematically planned ISA interventions such as structured campaigns using intranet messages or posters to educate employees and enhance their ISA. According to previous conceptual research, the most cost-effective method to prevent IS incidents is fostering ISA.

The purpose of this dissertation is to explore the role of ISA for promoting employees' ISP compliance. The four stages of this dissertation project focus on organizational efforts such as ISA programs to improve employees' compliant IS behavior and identifying predecessors for explaining employees' ISP compliance based on established scientific theories. A developmental mixed methods approach is conducted through these four stages of analysis. Primary data were collected in each stage to investigate banks operating in countries such as Austria, Germany, Czech Republic, Hungary, Slovakia, and Rumania.

In the first research stage, semi-structured expert interviews were conducted with operational risk and IS managers to explore banks' efforts to counteract IS incidents. The considered banks primarily use online methods such as intranet articles and conventional methods such as posters for building ISA. Second, the findings from stage one were incorporated in research stage two, in which a positivistic case study was conducted to test the Theory of Reasoned Action, Neutralization Theory, as well as the Knowledge-Attitude-Behavior model. The data were analyzed by utilizing partial least squares structural equation modeling (PLS-SEM). In addition to several qualitative interviews and an online survey at the headquarters of the case bank, data such as internal ISA materials (e.g., posters or IS intranet messages) were also analyzed. The second research stage provided empirical evidence that ISA program components affect employees' ISA, which further positively affects employees' attitudes and social norms toward compliance with ISPs, but negatively affects the use of neutralization techniques. All of these effects should eventually positively influence IS. This is shown in the chain of subsequent factors. The employees' attitudes and social norms positively affect the intention for compliant IS behavior, which is negatively affected by the use of neutralization techniques. In the third research stage, the influence of employees' perception of ISA programs on the Protection Motivation Theory was examined by conducting an online survey among German bank employees. It is demonstrated that employees' perception of ISA programs positively affects perceived severity as well as their coping mechanisms, which play the most important role in positively affecting the intention for compliant IS behavior. Surprisingly, employees' perception of ISA programs negatively affect perceived vulnerability. Moreover, perceived monitoring has a positive moderation effect on the intention-behavior link. Finally, the fourth research stage consists of a qualitative study to analyze the efforts of IS managers to enhance IS and examine how these efforts are perceived by users. Further, the inductive part of the study uncovers factors that influence the compliant IS behavior of users. Therefore, semi-structured interviews with IS managers were carried out to discover ISA program designs and categorize them according to design recommendations gained from current literature. In addition, this stage shows that individual ISP compliance seems to be connected with individual perceptions centering on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors.

To conclude, this dissertation provides several practical as well as theoretical contributions. From an academic perspective, the findings highlight the importance of attitudes, social norms, neutralization techniques, as well as coping mechanisms for employees' intentions to comply with their ISP. Future research might extend the findings by establishing and characterizing IS enhancing social norms and exploring methods of counteracting the common use of neutralization techniques. For practitioners, analysis of the design practices of ISA programs provides a better understanding of effectively using ISA interventions in the context of banks.

Zusammenfassung

Das Ziel dieser Dissertation ist die Rolle des Informationssicherheitsbewusstseins für die Einhaltung der organisationalen Richtlinien der Informationssicherheit zu erforschen. Die vierstufige empirische Studie identifiziert unter anderem Einflussfaktoren für das konforme Verhalten von Mitarbeitern hinsichtlich der Richtlinien der Informationssicherheit. Um die Mitarbeiter in Bezug auf Informationssicherheit zu sensibilisieren, haben Organisationen in der letzten Zeit strukturierte Programme zur Förderung der Informationssicherheit entwickelt und eingeführt. Diese Dissertation erforscht die Effekte der Implementierung von solchen Programmen zur Förderung der Informationssicherheit sowie die Effekte von Informationssicherheitsbewusstsein auf das konforme Verhalten der Mitarbeiter hinsichtlich der Richtlinien der Informationssicherheit mit Hilfe von etablierten wissenschaftlichen Theorien.

Die Vorgehensweise zur Untersuchung der Fragestellungen basiert auf einem Methoden Mix aus qualitativen und quantitativen Methoden. Die Forschung beruht auf vier Forschungsphasen und umfangreichen Primärdaten, die über Befragungen von Bankmitarbeitern aus Ländern wie Österreich, Deutschland, Tschechien, Ungarn, Slowakei oder Rumänien erhoben wurden. Zur Analyse der quantitativen Daten wurden varianzbasierte Strukturgleichungsmodelle aufgestellt und durch Testen korrelativer Zusammenhänge überprüft. Die qualitativen Daten wurden mittels thematischer Analyse untersucht.

In der ersten Phase wurden qualitative semi-strukturierte Interviews mit Experten aus dem operationalen Risiko- und Informationssicherheitsmanagement durchgeführt. Die untersuchten Banken nutzen verschiedene Methoden, wie z.B. Online-Kanäle wie Intranet-Nachrichten und konventionelle Methoden um Informationssicherheitsbewusstsein zu bilden. Die Ergebnisse der ersten Phase wurden in die zweite und dritte positivistische Forschungsphase eingearbeitet. In der zweiten Forschungsphase wurde eine Fallstudie ausgeführt, in der qualitative Interviews sowie eine quantitative Erhebung mittels Onlinefragebogen durchgeführt wurde. Die Fallstudie bediente sich der Theorie des Überlegten Handelns, der Neutralisierungstheorie sowie des Wissens-Einstellungs-Verhaltens Models. Es konnte nachgewiesen werden, dass das Informationssicherheitsbewusstsein einen großen Einfluss auf die Einstellungen, soziale Normen sowie auf das Neutralisierungsverhalten von Mitarbeitern hat. Die dritte Forschungsphase beruht zur Gänze auf einer quantitativen Online Befragung deutscher Bankmitarbeiter. Die Theorie der Schutzmotivation wurde angewendet um den Einfluss von Programmen zur Förderung des Informationssicherheitsbewusstseins zu untersuchen. Die Ergebnisse zeigen, dass aktuelle Programme zur Förderung des Informationssicherheitsbewusstseins eher die Bewältigungsmechanismen der Mitarbeiter stärken und relativ weniger die Bedrohungsbeurteilung ansprechen. Außerdem hat die wahrgenommene Überwachung einen Moderationseffekt auf den Zusammenhang zwischen der Absicht und dem aktuellen konformen Verhalten der Mitarbeiter hinsichtlich der Richtlinien der Informationssicherheit. Die vierte und letzte Phase dieser Dissertation besteht aus einer Fallstudie, die zunächst verschiedene Gestaltungsmöglichkeiten von Programmen zur Förderung des Informationssicherheitsbewusstseins vergleicht. Des Weiteren werden verschiedene Ansätze der untersuchten Fälle kategorisiert und Einflussfaktoren identifiziert, welche das Verhalten von Mitarbeitern der untersuchten Banken bezüglich der Konformität mit den Informationssicherheitsrichtlinien beeinflussen. Insgesamt wurden 33 qualitative Interviews mit Informationssicherheitsmanagern und Bankmitarbeitern geführt.

Die Dissertation bietet wichtige Einblicke sowohl für die betriebswirtschaftliche Praxis als auch für die wissenschaftliche Forschung bezüglich des Informationssicherheitsbewusstseins der Mitarbeiter. Die angewendeten Theorien wurden im Forschungskontext in neuen Zusammensetzungen bestätigt und die Ergebnisse heben die Bedeutung von Einstellungen, sozialen Normen, Neutralisierungsverhalten und Bewältigungsmechanismen für die Einhaltung der Informationssicherheitsrichtlinien hervor. Zukünftige Forschung könnte sich auf die Charakterisierung von sozialen Normen fokussieren, die Informationssicherheit verstärken und Neutralisierungsverhalten verhindern. Für Praktiker bietet die Analyse der Gestaltung von Programmen zur Förderung der Informationssicherheit besonderen Nutzen, da sie das Verständnis fördert, effektive Methoden zu gebrauchen.

1 Introduction

Organizations worldwide are confronted with a constantly increasing number of information security (IS) incidents (PricewaterhouseCoopers 2014). IS protects information resources of organizations by aiming to ensure the confidentiality, integrity, and availability of information (Dhillon 2007). Recently, IS incidents have been in the headlines of mass media, highlighting cases of leakage of millions of customers' data at well-known organizations, and in particular, banks (Marsden and Salmon 2015). Due to the pervasive nature of information and related technologies, data- and function-related IS incidents represent major threats for most types of businesses, as almost any processes and services may be negatively affected (Goldstein et al. 2011). Therefore, organizations are interested in finding solutions to prevent IS incidents and ensure IS (Siponen 2000). Some industries, such as the financial sector, rely even more heavily on well-functioning and secure information systems to survive in the competitive market (Goldstein et al. 2011). Confidentiality, integrity, and availability of information systems are absolutely necessary targets to guarantee data and information quality (Goldstein et al. 2011; Hsu et al. 2013b). Recent practitioner reports on IS incidents in banks show the increasing importance of enhancing IS (ORX 2014). In the last decade, bank regulators in particular have realized that much is at stake for banks and that professional management of IS is crucial to deal effectively with IS risks (Hsu et al. 2013).

To overcome this problem and to mitigate IS risks resulting from technology, processes, and human behavior, banks have introduced operational risk management, which is a regulatory requirement established by Basel II in 2004 (Hsu et al. 2013). Particular emphasis is drawn on quantification and measurement of operational risk (Goldstein et al. 2011). Banks have to cover these operational risks by forming reserves according to the three proposed measurement approaches. The advanced measurement approach is often used to calculate risk reserves and is based on loss data of the previous five years of the bank (Jobst 2007). Hence, banks are interested in minimizing their IS incidents to reduce their obligated capital reserves. Further, IS incidents may cause reputational damage as well (Gillet et al. 2010). For all these reasons, banks emphasize the prevention of IS incidents by introducing technological and behavioral controls.

Practitioners as well as researchers agree that technological solutions cannot ensure IS without considering the human threat (Crossler et al. 2013; Lebek et al. 2014). Employees' 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, might enable IS incidents (Siponen and Vance 2010; Stanton et al. 2005). Internal malicious coworkers or external perpetrators could benefit from employees' risk-taking behavior, because a toxic combination of risky behaviors can open possibilities to harm the bank (Guo 2013; Warkentin and Willison 2009). IS managers try to overcome employees' risk-taking behaviors by introducing information security policies (ISP) and ISA programs to increase employees' information security awareness (ISA).

ISA is defined as "a state where users in an organization are aware, ideally committed to, of their security mission" (Siponen 2000, p. 31). The main objective of ISA in an organizational context is to prevent individuals from risk-taking and malicious IS behaviors by enforcing organizations' ISP (Thomson and von Solms 1998). Therefore, ISA programs are introduced to address volitional and non-volitional risk-taking as well as malicious behaviors of employees through different kinds of ISA interventions such as conventional (e.g., posters, cups, handouts), online (e.g., intranet messages, e-learning) or instructor led (e.g., personal instructions) methods to enhance ISA . The thematic basis for organizational ISA programs is the ISP, which provides the baseline for mandatory organizational rules and offers guidelines as well as expected norms regarding the usage of information systems for employees to act desirable in terms of information security (Höne and Eloff 2002; Karyda et al. 2005). Previous scientific research discovered several factors from scientific theories that affect employees' compliance with organizational ISP (Bulgurcu et al. 2010; Ifinedo 2012), but still more empirical evidence on the socio-organizational perspective of ISA programs, and ISA and ISP compliance is needed (Crossler et al. 2013; Silic and Back 2014).

This dissertation aims to close the research gap by analyzing organizational ISA programs, individuals' ISA, and the eventual effects of both on compliant IS behavior. The dissertation builds on four research stages in the context of banks, in which certain aspects of ISA and ISA programs are investigated. The main scientific objectives are to explore organizational ISA efforts, to test positive and negative effects of ISA and ISA programs on employees' compliant IS behavior, and finally to discover ISA program design practices used

in practice. From a theoretical perspective, several theories such as Protection Motivation Theory, Theory of Reasoned Action, the Knowledge Attitude Behavior Model, and neutralization techniques are used to support the research models.

The thesis is composed in the form of a cumulative doctoral dissertation and is structured as follows. The next section introduces the research design and background, in which the research direction, including the integration of theories and a comprehensive overview of the research methodology, is presented. Afterward, the main results are shown and the findings are discussed. Following, the conclusion highlights the most important aspects and offers suggestions for future research. Finally, after the reference section, the appendix includes all relevant scientific articles of the cumulative dissertation.

2 Research Design and Background

2.1 Research Direction and Integration of Applied Theories

The general assumption of the dissertation is that organizational ISA programs might lead to an enhanced ISA of individuals, which finally might result in higher levels of ISP compliance. The assumed chain of factors is embedded in several theories throughout the single research stages. Figure 1 visualizes the proposed relationships of the main constructs of the dissertation.

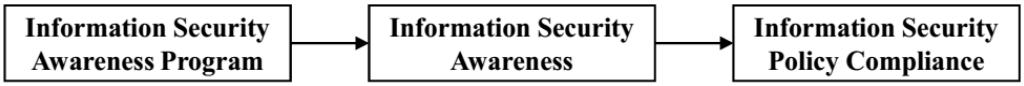


Figure 1: From ISA programs to ISA and finally to ISP compliance

Organizational efforts such as ISA programs are seen as the most cost-effective way to increase employees' ISA (Dhillon and Backhouse 2001). ISA programs are utilized to enhance employees' ISA regarding the content of banks' ISP, which introduce a binding standard concerning IS behaviors among all employees (Karyda et al. 2005). The main objective of ISA programs is to increase compliant IS behavior of employees to ensure IS such as the protection of confidential information (Thomson and von Solms 1998). In this research, all volitional or non-volitional risk-taking as well as malicious behaviors of employees are simply defined as employees' non-compliant IS behaviors, which refers to non-compliance with ISP of the researched organizations. However, social desirability often biases the assessment of response behavior (Ganster et al. 1983). We therefore follow recommendations to focus on compliant IS behavior as a dependent variable (Warkentin et al. 2012b).

Several deep-rooted scientific theories have been used to discover predecessors of employees' compliant IS behavior. Four popular theories often are used: the Protection Motivation Theory (PMT) (Herath and Rao 2009a; Son 2011; Vance et al. 2012), the General Deterrence Theory (GDT) (Cheng et al. 2013; D'Arcy and Herath 2011; D'Arcy et al. 2009; Hovav and D'Arcy 2012), the Technology Acceptance Model (Al-Omari et al. 2012a; Al-Omari et al. 2012b), and the Theory of Reasoned Action/Theory of Planned Behavior (TRA/TPB) (Sommestad and Hallberg 2013). After reviewing the scientific literature and reflecting on the research objectives, the TRA as well as the PMT were selected as the most promising theoretical lenses to shed light on individual employee behavior in connection with organizational IS efforts such as ISA programs. Figure 2 presents the integration of the applied scientific theories from research stage two and three in one theoretical model.

This dissertation applies a mixed method approach and answers a certain research question in each of the four different research stages. Because of the cumulative nature of the dissertation, for each research stage there are one or more completed articles which are also connected across the stages. The research questions are visualized in Table 1.

Research Stage	Research Questions
1	How do banks plan and implement ISA programs?
2	What are the effects of ISA on individual intentions for compliant IS behavior?
3	What are the effects of ISA programs on individual intentions for compliant IS behavior?
4	How do ISA program designs affect perceptions of employees in regard to compliant IS behavior?

Table 1: Research questions

As the first step, an explorative research question is raised to identify the organizational ISA practices and understand the specific banking context of the research. Previous conceptual articles mention that organizations introduce several different kinds of ISA interventions (Johnson 2006; Siponen 2000; Thomson and von Solms 1998). While literature offers comprehensive lists of ISA interventions (Johnson 2006) and categorizations of ISA interventions (Abawajy 2012), very limited information is available concerning the empirical evaluation of awareness programs in the context of banks and information security. Therefore, the main research objective is to discover how organizations actually plan and implement ISA programs to increase ISA of their employees.

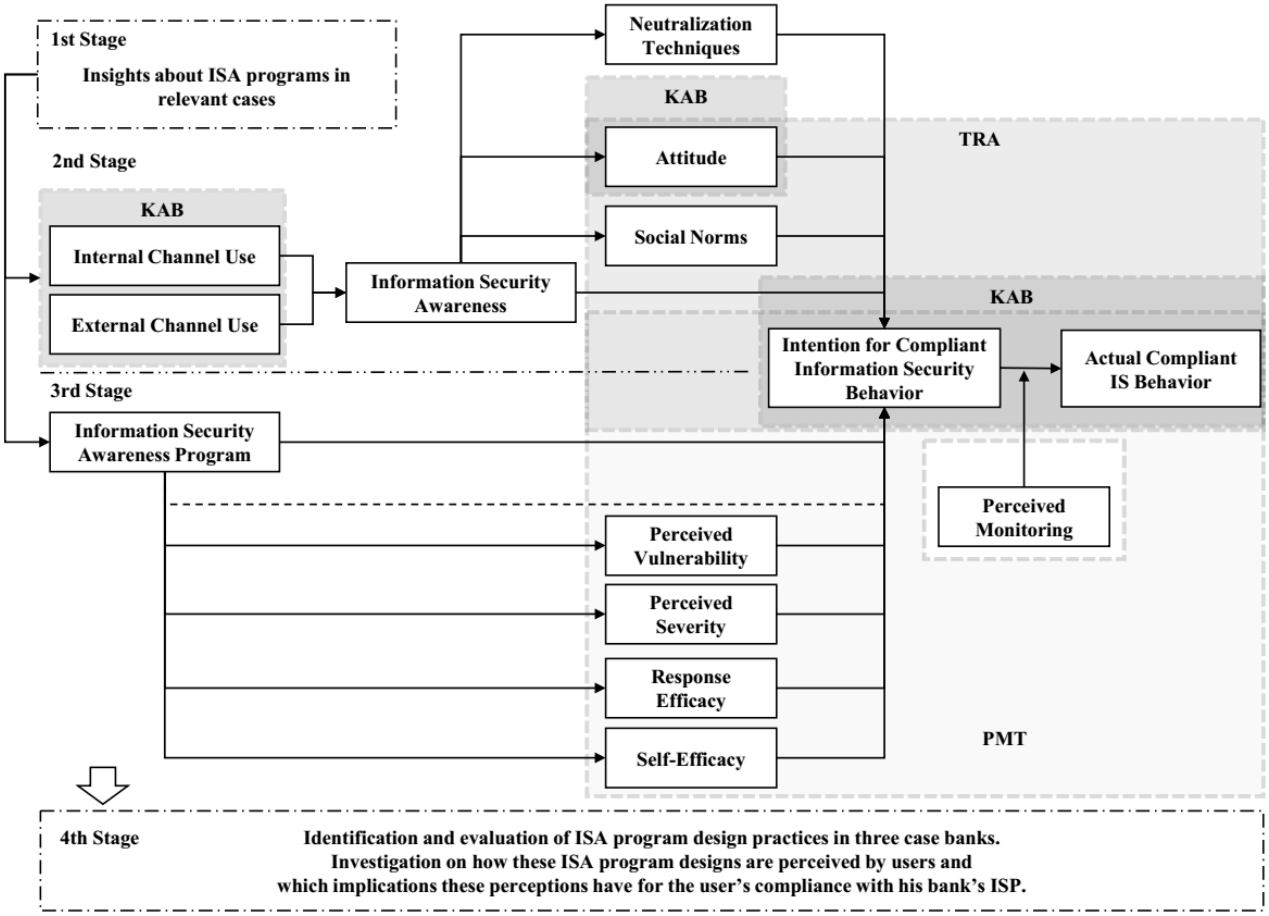


Figure 2: From ISA programs to ISA and finally to ISP compliance

The findings of the first research stage provided an important starting point for the next research stages. In the second research stage, the positivistic case study utilized a novel combination of the Theory of Reasoned Action (TRA), Neutralization Theory (NT), and the Knowledge, Attitude, Behavior (KAB) model to analyze which positive and negative effects ISA has on predecessors of employees' intentions for a compliant IS

behavior. The following paragraphs briefly introduce these theories and predecessors of intention for compliant IS behavior.

The TRA and the TPB are well-accepted psychological theories, which are heavily used to predict human behavior (Ajzen 1985; Ajzen 1991; Fishbein and Ajzen 1975). The TPB was applied among others in the research fields of health, safety, or advertising (Fishbein and Ajzen 2010). The TRA was originally found by Fishbein and Ajzen (1975), and the TPB is an extension of the original theory that incorporates the construct perceived behavioral control (Fishbein and Ajzen 2010). The TRA/TPB seems to fit perfectly to analyze individual behavior of employees in the ISP compliance context. In general, recent academic research used the TRA/TPB (Cox 2012; Siponen et al. 2010), but particularly the perception of organizational efforts such as ISA programs have not been applied in research models in connection with TRA/TPB. All in all, there is empirical evidence for the importance of the antecedents "attitude" and "social norms" for the intention for compliant IS behavior (Sommestad and Hallberg 2013). The dissertation yields a deeper understanding of the effects of interventional factors (e.g., internal and external information use abstracted from ISA programs) on the constructs "attitude" and "social norms'" Further, the impact of "attitude" and "social norms" on employees' ISP compliance behaviors is tested.

NT were first mentioned by Sykes and Matza (1957) to explain the deviant behavior of adolescents in the 1960s. In essence, the techniques are used by people to justify and excuse their deviant behavior for themselves and possibly others (Sykes and Matza 1957). In the past decades, NT was established as a criminology theory, but it was also used in health (Maruna and Copes 2004) or ISP compliance research (Barlow et al. 2013; Siponen and Vance 2010). The latter calls for more research in this area, because Barlow et al. (2013) showed that some justifications by means of certain techniques of neutralization are more important than others in different types of research contexts (e.g., defense of necessity for password security). Five techniques of neutralization have been originally introduced by Sykes and Matza (1957), but scientific research identified an additional four techniques over the decades of research (Maruna and Copes 2004). For the specific research context of this study, the adequacy of certain neutralization techniques was checked by conducting interviews with IS managers in advance. Hence, through this research, the neutralization techniques "condemnation of the condemners," "defense of necessity," "denial of responsibility," and "denial of injury" were analyzed.

The KAB model summarizes the process of change in behavior triggered by changes in attitude-relevant knowledge (Chaffee and Roser 1986). The basic idea is that, first, attitude-relevant knowledge is absorbed by the individual; this is followed by attitude-relevant beliefs as well as the attitude itself, and finally in the last step by compliant IS behavior of the individual change. Especially in the ISP compliance context, previous literature shows that ISP knowledge influences how intentions for compliant information security behavior are formed (Pahnila et al. 2013). Organizations plan to deliver attitude-relevant knowledge to their employees by ISA programs, which should be designed carefully to understand their overall levels of effectiveness in fulfilling their purpose (Albrechtsen and Hovden 2010; Hagen et al. 2011). Knowledge is represented by internal and external channel use, and attitude and behavior is conceptualized as it is provided by other theories.

The third research stage used the Protection Motivation Theory (PMT) to examine which positive and negative effects ISA programs have on predecessors of intention for a compliant IS behavior. The PMT was originally introduced by Rogers et al. (1975) and offers a theoretical view on motivational influences on the intention for a certain behavior (Rogers et al. 1983). The underlying dissertation utilized the PMT in the same way as recent state-of-the-art IS research (Ifinedo 2012). The theory builds on coping as well as threat appraisals. The latter consists of perceived vulnerability and perceived severity. In this research, perceived vulnerability is defined as an individual's perception of the probability of an information security incident, which is caused by behavioral non-compliance with the ISP. Further, perceived severity reflects the impact of an information security incident caused by non-compliance with the ISP. Besides the threat appraisal, the coping appraisal consists of response efficacy and self-efficacy. Response efficacy is defined as the expectancy of the employee that the threat or risk can be mitigated by conducting the ISP compliant security behavior. Finally, yet importantly, the construct self-efficacy is the belief that one is able to conduct the requested behavior for compliance. The PMT is heavily used in many studies and, especially in the behavioral IS compliance context, the PMT has received significant recognition (Lebek et al. 2014).

The final research stage addresses the questions, "Which ISA program designs recommended by scientific research are used in practice?" and "How do these implemented designs affect employees' compliant IS behavior?" Through this study, the research aims to go beyond established ways of explaining compliant IS behavior by offering view of the IS managers as well as users about ISA programs and ISP compliance. Previous qualitative research largely neglected to investigate ISA programs and their effects in depth (Albrechtsen 2007; Posey et al. 2014). Further, ISA program designs have only been analyzed as single ISA interventions (Kajzer et al. 2014; Shaw et al. 2009). Therefore, the study provides a more nuanced understanding in terms of how IS managers structure and communicate ISA interventions of an ISA program and how employees' perceive organizational practices such as ISA programs to increase ISA.

2.2 Mixed Methods Research Design

The research utilizes a developmental mixed methods design, which supports the thesis by offering a holistic view of the research problem and offering theoretically plausible answers to the research questions (Venkatesh et al. 2013). The developmental mixed methods design provides several benefits for the study: First, the triangulation of research methods presents a holistic picture of the research context. Particularly, in this case, the banking context is important to discover because regulations and legislations triggered changes in the past decade. Second, the use of multiple research methods is beneficial as it helps to overcome the shortcomings and biases such as the common method bias (Venkatesh et al. 2013). Overall, the results of the four research stages taken together offer a comprehensive picture of ISA and ISP compliance.

The full research process consists of a pre-stage and four main research stages, which are visualized by Figure 3. In terms of data collection, the empirical studies used interview data, quantitative data received by online surveys, as well as internal documents of the organizations such as ISA intranet messages, posters, cups, or internal documents. From an organizational perspective, the research units are banks from Central and Eastern European (CEE) countries, which differ from stage to stage. From an individual perspective, in each research stage, data were collected by interacting with bank employees. Most insights are achieved by applying quantitative or qualitative research methods on bank employees. An overview of the main methodological aspects of the four research stages are summarized in Table 3.

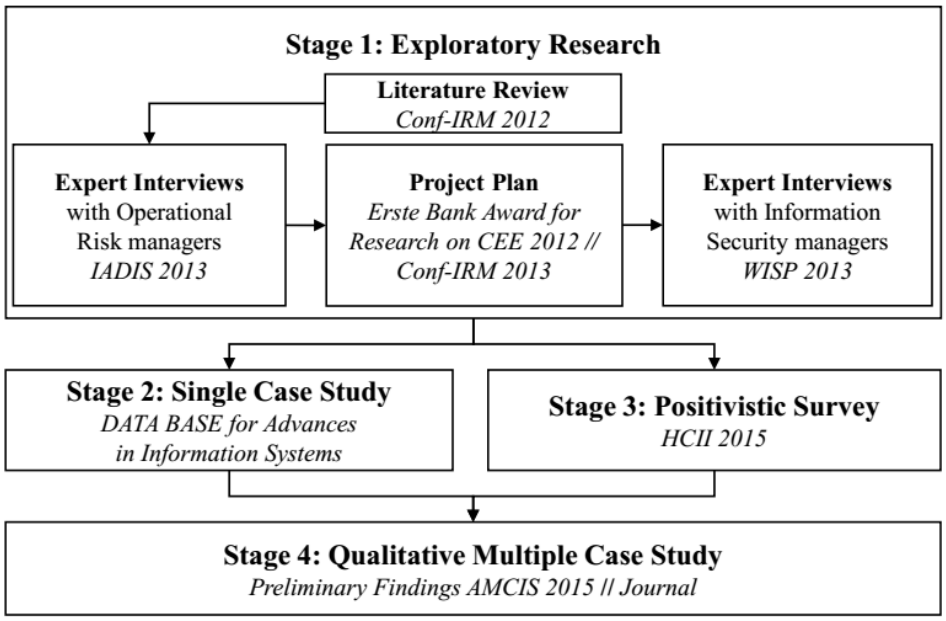


Figure 3: Research methodology (Mixed Methods Triangulation approach; publications written in *italics*)

At the beginning, a comprehensive literature review was conducted to obtain insights on the latest scientific advances (Bauer 2012). Afterward, first experts in the field of operational risk were selected through the snowball technique and through an online social network search to conduct initial semi-structured interviews, which explored the research context in banks and led to a first publication of the results (Bauer and Bernroider 2013b). Next, a project plan was developed with the commitment of one of the interviewees and submitted to acquire third-party funding. After the project plan was accepted, a project kick-off workshop started to

identify further potential areas for research. The findings of this process also were presented in a research-in-progress conference publication (Bauer and Bernroider 2013a). Finally, qualitative expert interviews with information security managers were conducted to explore ISA programs in more detail (Bauer et al. 2013a). A thematic analysis was used to analyze the semi-structured interviews (Braun and Clarke 2006). Overall, the first research stage was important for identifying the research interests and supporting the development of research hypotheses for the next stages of theory testing research.

In research stage two, a positivistic case study based on a single case for theory testing purposes was conducted to confirm and extend existing theories in the context of a large bank organization (Eisenhardt 1989; Yin 2009). In particular, pre-survey data were collected through four initial face-to-face interviews with certain managers of the bank to obtain more insights about the specific research context. Next, the survey phase started with three rounds of pre-testing. After that, the case organization's chief information security officers approved the survey before it went online for two weeks at the headquarters of the bank. Next, the data were analyzed with partial least squares structural equation modeling (PLS-SEM) according to the guidelines provided by Hair et al. (2014). The research model consists of reflective as well as formative constructs, hence validity checks and the measurement model have been adopted accordingly.

There are several reasons why PLS-SEM was used. First, the measurement and the structural model can be analyzed at once (Hair et al. 2011). Second, the decision for PLS-SEM is due to the research aim, which is to explain the variance of the endogenous construct "intention for compliant employee security behavior" (Sarstedt et al. 2011). Third, PLS-SEM can be utilized for small sample sizes (Hair et al. 2011).

	Stage 1: Exploratory Research	**Stage 2: Single Case Study**	**Stage 3: Positivistic Survey**	**Stage 4: Qualitative Multiple Case Study**
Description of the method(s)	Qualitative content analysis of semi-structured expert interviews	Qualitative Interviews, PLS-SEM (Partial Least Squares Structural Equation Modeling)	PLS-SEM (Partial Least Squares Structural Equation Modeling)	Qualitative content analysis of semi-structured interviews with IS managers and users
Philosophical perspective	Interpretative	Positivistic	Positivistic	Interpretative
Research unit	8 bank groups (4 national, 4 international)	1 bank group (headquarter employees)	Not defined number of banks in Germany	3 bank groups (international, headquarter, and branch employees)
Participants	8 operational risk and 6 information security managers	97 bank employees	183 bank employees	33 interviews with bank employees

Table 3: Research Stages According to the Triangulation of Methods

Similar to the second stage, the third research stage also applied a positivistic theory-testing and quantitative approach. For data collection, a German crowed sourcing platform was consulted to conduct an online survey of German bank employees. This phase of the research enabled collection and analysis of data from a sizable sample size to capture a large bandwidth of ISA programs to study their differing effects on employees' compliance with ISP. PLS-SEM was used for data analysis (Hair et al. 2014). Contrary to the second research stage, the research model was developed as a fully reflective measurement model. All quality criteria are within the required limits.

The survey instruments in research stage two and three were developed by screening state-of-the-art literature for similar construct definitions for finding well-established psychometric properties of management information systems instruments. Nonetheless, recommended validity and reliability checks were conducted, and special attention was given to internal construct validity, which was ensured by data source and between-method triangulations by using multiple sources of data for the same issues (e.g., by interviewing different managers about ISP compliance and using different data collecting methods such as survey, interviews, and documents). The bootstrap re-sampling procedure was used to test the significance of all model paths (Sarstedt et al. 2011).

In the fourth research stage, a multiple case study design (Cavaye 1996; Yin 2009) was used to investigate three units of analysis, in particular three banks from Central and Eastern Europe. In total, 33 interviews were conducted, distributed in 23 interviews with users and 10 interviews with IS managers. Further, materials of ISA programs, such as intranet messages and posters, were analyzed. Each bank was selected by focusing on a contrasting case study design (Stake, 2005) to evaluate ISA programs that cover design recommendations by scientific literature. After transcribing all interviews, content analysis was used to develop first- and second-order categories (Huberman and Miles 1994; Mayring 2003). After each round of coding, the codes were checked and discussed.

3 Summarized Results and Discussion of the Main Findings

The cumulative nature of this dissertation requires that the underlying scientific articles are combined to a coherent dissertation, building on several connected research questions through the research stages. All in all, this dissertation comprises eight peer-reviewed academic articles, which are or will be published in academic conference proceedings or high-quality academic journals. The peer-review process ensures that the articles are critically evaluated by the scientific community to confirm the quality of the work done. Therefore, the cumulative dissertation ensures high-quality research standards, reflects the acknowledgment of the scientific community, and increases the impact of the dissertation by disseminating subsections of the dissertation via conference proceedings and journals. In the following subsections, the results and findings of each completed research stage are presented and discussed in detail.

The main contribution of the dissertation addresses organizational ISA programs, employees' ISA, as well as their compliance with the ISP. In total, the dissertation contributes to theoretical (Dhillon and Backhouse 2001; Lebek et al. 2014), practical (Wilson and Hash 2003), qualitative (Albrechtsen 2007; Albrechtsen and Hovden 2009; Posey et al. 2014), quantitative (Bulgurcu et al. 2010; Herath and Rao 2009b; Hu et al. 2012; Siponen et al. 2014), and conceptual (Johnson 2006; Siponen 2000; Thomson and von Solms 1998) literature of the past decades on behavioral ISP compliance research. A summary of the most important findings is presented in Table 4. The results of quantitative data analysis of the theory testing research stages two and three are summarized in Figure 4.

	Stage 1: **Exploratory Research**	**Stage 2:** **Single Case Study**	**Stage 3:** **Positivistic Survey**	**Stage 4:** **Qualitative Multiple Case Study**
Main Contribution regarding **ISA Programs**	Categorization of banks' ISA interventions in conventional, online, and instructor-led methods. Result: most ISA programs consists of basic online methods (e.g., intranet articles, e-learning). No control of the effectiveness of the ISA interventions.	Relatively more important: 1. Internal online channels (e-learning, intranet messages). 2. Conventional methods (newspapers, posters, and leaflets). Relatively less important: 1. Instructor-led trainings 2. Informal talks. ISA programs explain a significant part of employees' ISA, but external information use is relatively more important.	Employees' perceptions of ISA programs are relatively most important for influencing: 1. Self-efficacy (positive) 2. Response efficacy (positive) 3. Perceived vulnerability (negative) 4. Perceived severity (positive) 5. Intention for a compliant IS behavior (positive)	Evaluation of the occurrence of structural and communicational ISA program design practices; important are: media richness, implementation of the full cycle, non-technocratic IS risk communication, feedback interventions, use of role plays, and enforcement of reflection and dialog. Identification of ISA program approaches (interaction, incident-related, accountability approach).
Main Contribution regarding **ISA**	-	ISA explains the most variance of employees' attitude and subjective norms. ISA counteracts neutralization techniques.	-	Different groups of employees (such as headquarter or branch employees) have differing specific needs and requirements regarding ISA and ISA interventions.
Main Contribution regarding **ISP Compliance**	Actual topics regarding banks' ISP were implemented in ISA programs. No behavioral controls of employees' compliance with ISP.	Relatively most important for affecting employees' intentions for compliant IS behavior: 1. Attitude 2. Social norms 3. Neutralization techniques.	Relatively most important for affecting intention for compliant IS behavior: 1. Response efficacy 2. Self-efficacy 3. Perceived severity 4. ISA programs (all factors are positive) Perceived vulnerability has no effect on intention for compliant IS behavior. Perceived monitoring has a positive moderating effect on the intention-behavior link.	Certain coverage levels of ISA program designs address the users' perceptions of IS risks, knowledge of the ISP, their perception of responsibility regarding ISP, their perception of importance of ISP compliance, and the use of neutralization techniques to justify misbehavior.

Table 4: Research Stages and Findings

3.1 Stage 1: Exploratory Research

The manuscripts representing this sub-section:

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

Bauer, S., and Bernroider, E. W. N. 2013a. "It Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.

Bauer, S., and Bernroider, E. W. N. 2013b. "It Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, Miguel Baptista Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2013. "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

The literature review identifies research gaps of the recent academic literature in the area of IT operational risks in the context of financial institutions. The analysis included 37 scientific articles that address financial institutions, regulations such as Basel II, and IT operational risk. The findings show that research on people and organizational complexity in the context of IT operational risk was neglected by scientific literature.

After the literature review, semi-structured expert interviews were conducted with IT operational risk experts and with IS managers. First, interviews with four IT operational risk managers from four banks resulted in initial insights about the banks' efforts to reduce incidents resulting from information technology, processes, and human behavior. IT operational risk awareness was a topic in each bank, because banks installed responsible persons for building awareness. In particular for IT related issues, ISA programs were conducted by IS managers; therefore, the research moves on to ask them.

Next, the evaluation of the ISA programs of five banks was conducted through ten semi-structured interviews with IS managers. Compared to recent suggestions by academic literature (Johnson 2006; Wilson and Hash 2003), the researched banks primarily use very basic ISA interventions, such as intranet articles, leaflets, and posters. Interestingly, all research units utilize E-learning concerning ISP compliance at organizational entry or on a yearly basis. The banks require their employees to go through an E-Learning program for general compliance, in which IS and the ISP is a part. Finally, all employees have to pass an exam. Most of the banks investigated in the study mix several ISA interventions, but they do not follow a clear strategy for how to raise employees' ISA. The measurement of the effectiveness and the controls of the methods only exist on a very general level and focus on knowledge repetition (e.g., quizzes, exams). Based on the findings, the cornerstones for the surveys for discovering the positive and negative effects of ISA and ISA programs on employees' IS behavior have been laid.

3.2 Stage 2: Single Case Study

The manuscript representing this sub-section:

Bauer, Stefan, Bernroider, Edward W.N.. „From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization," *The DATA BASE for Advances in IS* (accepted as research article).

The second research stage consists of a case study, in which qualitative data in the form of semi-structured interviews as well as quantitative data in the form of an online survey in the headquarter of an Austrian bank have been collected. The findings of the first stage are incorporated in the theoretical model, in which a causal chain leads from internal and external channel use for information acquisition to employees' intentions for

compliant IS behavior. Internal channel use reflects ISA programs, and this was neglected by scientific literature until now. The main theoretical contribution of this research stage is that state-of-the-art literature is extended by discovering positive or negative effects of constructs in the causal chain of latent variables on employees' intentions for compliant information security behavior. The impact of internal and external IS information has not been adequately addressed until now. Instead of testing a direct link from ISA to intention for a complaint IS behavior, the theoretical model integrates the Theory of Reasoned Action (TRA), the Knowledge, Attitude, Behavior (KAB) model, and neutralization techniques (NT) to understand how compliant information security behavior emerges in a large bank.

In general, all paths are significant, and therefore the proposed research model was fully supported by the data. The study shows that internal as well as external channel use significantly affect employees' ISA. This finding supports previous research that information processing is a pre-condition for changing behavior (Fishbein and Ajzen 1975) and provides empirical evidence for the importance of the KAB model in this context. In terms of internal ISA interventions, internal online channels (e.g., e-learning, intranet messages) and conventional methods (newspapers, posters, and leaflets) are relatively more important than instructor-led trainings and informal talks with colleagues. For external channel use, self-organized learning as well as classic media are relatively more important than online media and informal talks with family and friends. As a practical implication, banks may actively endorse the use of external information sources by providing a weekly media digest linking to IS incidents.

Further, there is empirical evidence that ISA has a significant influence on all three proposed predictors of intention for a compliant IS behavior. ISA has a strong positive effect on attitude, a moderate positive effect on social norms, and a weak negative effect on neutralization techniques. This result highlights the importance of ISA and thereby confirms previous empirical (Albrechtsen and Hovden 2010; Bulgurcu et al. 2010; Eminağaoğlu et al. 2009; Hagen et al. 2011) and conceptual (Siponen 2000; Thomson and von Solms 1998) studies on emphasizing the significance of ISA.

Next in the chain of factors, all proposed constructs of TRA and neutralization techniques significantly affect employees' intentions for complaint IS behavior. Attitudes toward a compliant IS behavior seem to be most important in relative terms. Interestingly, attitude was also found as most important by Siponen et al. (2014a), but in contrast, certain studies (Bulgurcu et al. 2010; Herath and Rao 2009b; Hu et al. 2012) in the ISP compliance context reported other constructs as relatively more important. The difference could be due to the research sample, because instead of using a real-life bank case, other studies targeted students (Hu et al. 2012) or mixed professionals (Bulgurcu et al. 2010; Herath and Rao 2009b).

The results extend existing literature by showing that neutralization techniques are slightly more important than social norms, considering the fact that both variables have a weak effect on the endogenous variable. Consistent with previous research (Barlow et al. 2013), some neutralization techniques are more powerful than others, depending on the research context. As a practical implication regarding the neutralization technique "condemnation of the condemners," IS managers should only introduce ISP that are perceived as reasonable and fair. In terms of "defense of necessity," employees could be reminded that urgent work and deadlines are no valid justifications for ignoring the ISP.

Last, but not least, social norms that have a weak positive effect on the intention for a complaint IS behavior are an indicator for the impact of the social environment (Herath and Rao 2009a; Herath and Rao 2009b) on employees' ISP compliance. It is assumed that a strong IS culture forces employees to comply (Merhi and Midha 2012; Van Niekerk and Von Solms 2010), and following IS managers might proactively enhance social norms by appointing ambassadors of IS among the workforce (Guo 2013).

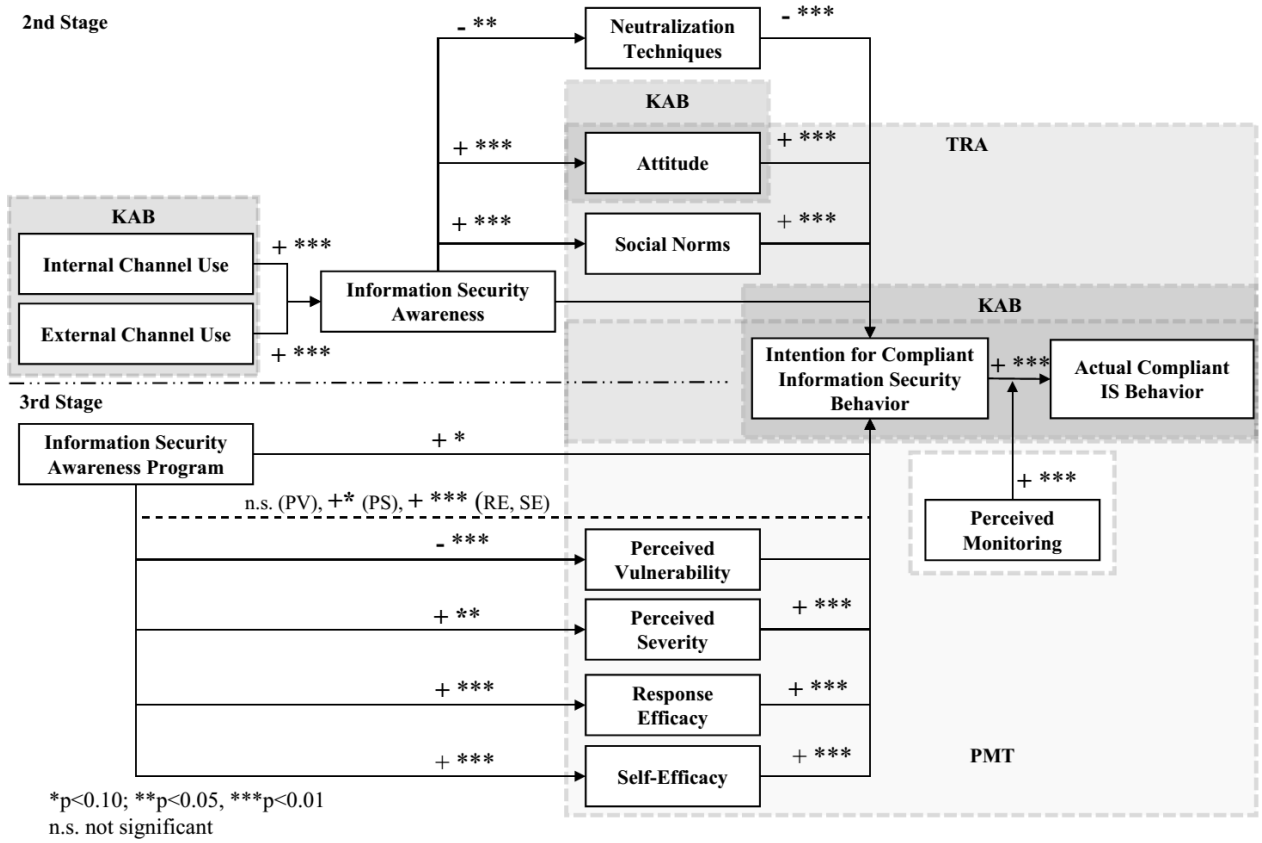


Figure 4: Results from theory testing research stages

3.3 Stage 3: Positivistic Survey

The manuscript representing this sub-section:

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust*, 154-164, Hrsg. Los Angeles.

In research stage three, the study aims to analyze how employees' perceptions of ISA programs influence their protection motivation. Therefore, a causal chain of factors was applied to examine employees' intentions for compliant IS behavior by considering coping and threat appraisals as well as employees' perceptions of ISA programs. Finally, yet importantly, the moderation effects of organizational monitoring on the intention-behavior link have been tested.

First in the chain of factors, ISA program have a moderate effect on response and self-efficacy, which confirms the important role of ISA programs to introduce coping mechanisms. In contrast, ISA programs have only a weak positive effect on perceived severity and, surprisingly, a weak negative effect on perceived vulnerability. Moreover, ISA programs have a weak direct effect on intention for compliant IS behavior, but the mediation analysis also confirms that three constructs (perceived severity, response efficacy, and self-efficacy) act as mediators. Overall, this study contributes to conceptual (Johnson 2006; Siponen 2000) and practical (Wilson and Hash 2003) literature by confirming that the perceptions of ISA programs positively affect employees' intentions for compliant IS behavior.

According to the results, the response efficacy and self-efficacy affect the individuals' intentions for compliant IS behavior relatively more than the threat appraisals' constructs. This finding confirms previous research (Ifinedo 2012; Meso et al. 2013), but also contradicts a study of Siponen et al. (2014). Reflecting on the results, it seems that ISA programs are relatively more successful in offering coping actions than actually increase employees' perceptions about vulnerability and severity of threats. Hence, employees who believe that they can mitigate IS risks might have a higher intention to act according to the ISP.

In contrast to other predecessors of intention, ISA programs have a negative influence on perceived vulnerability, which further has no effect on intention for a compliant IS behavior. Astoundingly, prior research found positive effects and therefore conflicting results for the relationship of perceived vulnerability and intention for compliant IS behavior (Ifinedo 2012; Siponen et al. 2014). Environmental or contextual factors might distort this result (Hu et al. 2012; Padayachee 2012; Tsohou et al. 2013). To conclude, employees might not connect ISP content with real danger.

Organizational monitoring shows a partial positive moderation effect on the well-established causal relationship of intention for a compliant IS behavior and actual IS behavior. As a practical implication, it can be recommended that ISA programs should inform employees about organizational monitoring. Furthermore, ISA programs should provide better communication about the occurrence of real threats from media or inside the company.

3.4 Stage 4: Qualitative Multiple Case Study

The manuscripts representing this sub-section:

Bauer, Stefan, Chudzikowski, Katharina. 2015. „Mind the Threat! A Qualitative Case Study on Managing Information Security Awareness Programs in Central and Eastern European Banks," In *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Hrsg. Allen Lee, Puerto Rico.

Bauer, Stefan, Chudzikowski, Katharina, Bernroider, Edward. „Prevention is better than Cure! Designing Information Security Awareness Programs to Overcome the Security Digital Divide in CEE Banks" (submitted as research article).

The fourth and final research stage is divided in the investigation of ISA program designs and their influences on employees' IS behavior in organizations. First, IS managers' efforts were researched by comparing design recommendations from IS literature with actual ISA program design practices in three banks. Second, qualitative interviews of users of the case banks are conducted to abstract influencing factors for ISP compliance. Finally, coverage levels of ISA program design recommendations are combined with influencing factors for ISP compliance.

To date, previous research discussed mostly single ISA program designs (Kajzer et al. 2014; Shaw et al. 2009) and neglected a holistic view on ISA programs. Hence, as a first step, a literature review was conducted to summarize and categorize all findings from academic literature about ISA program designs. The design recommendations are categorized in communicational and structural aspects. Afterward, the design recommendations abstracted from recent scientific literature and actual practices in three CEE banks were compared. Alpha bank implemented nearly all of the design recommendations in its ISA program. Alpha bank showed that design recommendations, such as media richness (Shaw et al. 2009), implementation of the full cycle (Wilson and Hash 2003), non-technocratic IS risk communication (Clarke et al. 2012), feedback interventions (Eminağaoğlu et al. 2009), use of role plays (Karjalainen et al. 2013a), and enforcement of reflection and dialog (Albrechtsen and Hovden 2010), can be combined to a comprehensive ISA program. However, further analysis distinguishes between high and low coverage of design recommendation, because in contrast to Alpha bank, the other two banks covered only a few design recommendations. The researched banks applied approaches that can be categorized as the interaction, the incident-related, and the accountability approach.

Next, empirical data were obtained by qualitative interviews with users of the case banks to abstract influencing factors for ISP compliance, which consists of perceptions centering on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors. Perceptions of responsibilities regarding ISP compliance differ heavily between certain stakeholders because of different levels of perceived importance and knowledge about the ISP. Employees working in banks' headquarters or branches are not recognizing their importance in ensuring organizations' IS. Further, they do not have the necessary knowledge of banks' ISP to know all responsibilities. This finding extends existing research by providing deep insights in branch-headquarter aspects (Albrechtsen 2007; Albrechtsen and Hovden 2009; Kolkowska 2011a; Posey et al. 2014).

Neutralization techniques are used by employees to justify intentional violations of banks' ISP (Barlow et al. 2013; Siponen and Vance 2010). The results show that well-covered ISA programs diminish partially the use of neutralization techniques. Employees reported some well-known neutralization techniques, but astoundingly branch employees are using more techniques such as "appeal to higher loyalties" and "defense of necessity" (Siponen and Vance 2010) compared to headquarter employees. Branch as well as headquarter users utilize the technique "denial of injury."

The findings extend previous qualitative research on ISA and ISA programs (Albrechtsen 2007; Albrechtsen and Hovden 2009; Posey et al. 2014) by confirming both the theoretical and practical relevance of organizational efforts such as ISA programs for increasing employees' ISP compliance. The findings offer several practical implications. First, scientific design recommendations should be considered for effective and innovative ISA programs. In particular, the design practice "emotional involvement" of employees seems to be beneficial to achieve a dialog between employees. This can be implemented by using role plays or quizzes. Second, ISA programs suffer from a lack of evaluation mechanism. Therefore, plan, do, check, act cycle models with an evaluation mechanism should be introduced to enforce strategic planning. Third, the needs and requirements of single stakeholders regarding ISP compliance should be evaluated to raise understanding for all stakeholder groups and design ISA programs by customizing mass media interventions. Fourth, the neutralization techniques "denial of injury," "appeal to higher loyalties," and "defense of necessity" are highly relevant in the research context, and hence practitioners should tackle these techniques in their ISA programs.

4 Conclusion

The findings of the underlying dissertation demonstrate that ISA plays an important role in promoting ISP compliance. The findings show that the consumption of well-designed organizational ISA programs increases the individuals' ISA, which is likely to increase their ISP compliance. The study contributes to existing behavioral IS research by highlighting the importance of attitudes, social norms, neutralization techniques, perceived severity, response efficacy, and self-efficacy for explaining employees' intentions for compliant IS behavior. Additionally, the research designs provide evidence for the adequacy of applying and combining the considered theories (TRA, NT, KAB model, and the PMT) for analyzing employees' compliant IS behaviors. The dissertation offers important implications with regard to ISA programs, as previous literature has largely neglected to explore ISA programs in practice. Further, it was investigated how different coverage levels of ISA program designs recommended by literature affect employees' perceptions centering on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors.

Throughout the four research stages, qualitative as well as quantitative methods were applied to obtain a holistic overview of the research problem. The developmental mixed methods approach is beneficial to overcome shortcomings of single research methods and provides an in-depth discussion of the overall research objectives. Empirical data have been collected at several banks in CEE. Special emphasis was given to evaluate research quality criteria such as validity and reliability. The study contributes to the context of banks in CEE, and findings cannot be generalized for other research contexts.

Future research should emphasize developing and testing sophisticated ISA controls on employees' IS behaviors. In particular, future research may focus on single neutralization techniques in more detail and connect neutralization theory with social climate research. Moreover, more applied research (e.g., action research) could explore the effectiveness of innovative ISA interventions such as viral videos and serious games to improve employees' compliant IS behaviors.

References

Abawajy, J. 2012. "User Preference of Cyber Security Awareness Delivery Methods," *Behaviour & Information Technology* (33:3), pp. 237-248.

Ajzen, I. 1985. "From Intentions to Actions: A Theory of Planned Behavior," in *Action-Control: From Cognition to Behavior* J.K.J. Beckman (ed.). Heidelberg: Springer, pp. 11-39.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Al-Omari, A., El-Gayar, O., and Deokar, A. 2012a. "Information Security Policy Compliance: The Role of Information Security Awareness,").

Al-Omari, A., El-Gayar, O., and Deokar, A. 2012b. "Security Policy Compliance: User Acceptance Perspective," *System Science (HICSS), 2012 45th Hawaii International Conference on*: IEEE, pp. 3317-3326.

Albrechtsen, E. 2007. "A Qualitative Study of Users' View on Information Security," *Computers & Security* (26:4), pp. 276-289.

Albrechtsen, E., and Hovden, J. 2009. "The Information Security Digital Divide between Information Security Managers and Users," *Computers & Security* (28:6), pp. 476-490.

Albrechtsen, E., and Hovden, J. 2010. "Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study," *Computers & Security* (29:4), pp. 432-445.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce It Policy Violation," *Computers & Security* (39), pp. 145-159.

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, R.J. Brandtweiner (ed.), Vienna, pp. 1-14.

Bauer, S., and Bernroider, E. W. N. 2013a. "It Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM 2013)*, L. Janczewski (ed.), Natal, pp. 1-4.

Bauer, S., and Bernroider, E. W. N. 2013b. "It Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013*, P.I.a.P.P. Miguel Baptista Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2013. "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

Braun, V., and Clarke, V. 2006. "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* (3:2), pp. 77-101.

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), pp. 523-548.

Cavaye, A. L. M. 1996. "Case Study Research: A Multi-Faceted Research Approach for Is," *Information Systems Journal* (6:3), pp. 227-242.

Chaffee, S. H., and Roser, C. 1986. "Involvement and the Consistency of Knowledge, Attitudes, and Behaviors," *Communication Research* (13:3), pp. 373-399.

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), pp. 447-459.

Clarke, N., Stewart, G., and Lacey, D. 2012. "Death by a Thousand Facts," *Information Management & Computer Security* (20:1), pp. 29-38.

Cox, J. 2012. "Information Systems User Security: A Structured Model of the Knowing–Doing Gap," *Computers in Human Behavior* (28:5), pp. 1849-1858.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90-101.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Dhillon, G. 2007. *Information Systems Security*. Susan Elbe.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of Management Review* (14:4), pp. 532-550.

Eminağaoğlu, M., Uçar, E., and Eren, Ş. 2009. "The Positive Outcomes of Information Security Awareness Training in Companies – a Case Study," *Information Security Technical Report* (14:4), pp. 223-229.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior*. Reading, MA: Addison-Wesley.

Fishbein, M., and Ajzen, I. 2010. *Predicting and Changing Behavior: The Reasoned Action Approach*. Psychology Press, Taylor & Francis Group.

Ganster, D. C., Hennessey, H. W., and Luthans, F. 1983. "Social Desirability Response Effects: Three Alternative Models," *Academy of Management Journal* (26:2), pp. 321-331.

Gillet, R., Hübner, G., and Plunus, S. 2010. "Operational Risk and Reputation in the Financial Industry," *Journal of Banking & Finance* (34:1), pp. 224-235.

Goldstein, J., Chernobai, A., and Benaroch, M. 2011. "An Event Study Analysis of the Economic Impact of It Operational Risk and Its Subcategories," *Journal of the Association for Informaton Systems* (12:9), pp. 606-631.

Guo, K. H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," *Computers & Security* (32), pp. 242-251.

Hagen, J., Albrechtsen, E., and Johnsen, S. O. 2011. "The Long-Term Effects of Information Security E-Learning on Organizational Learning," *Information Management & Computer Security* (19:3), pp. 140-154.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2014. *A Primer on Partial Least Squares Structural Equation Modeling (Pls-Sem)*. Thousand Oaks: SAGE Publications Ltd.

Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. 2011. "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," *Journal of the Academy of Marketing Science* (40:3), pp. 414-433.

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

Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Höne, K., and Eloff, J. H. P. 2002. "Information Security Policy—What Do International Information Security Standards Say?," *Computers & Security* (21:5), pp. 402-409.

Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. And South Korea," *Information & Management* (49:2), pp. 99-110.

Hsu, C., Backhouse, J., and Silva, L. 2013. "Institutionalizing Operational Risk Management: An Empirical Study," *Journal of Information Technology*).

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-659.

Huberman, A. M., and Miles, M. B. 1994. "Data Management and Analysis Methods,").

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), pp. 83-95.

ISACA. 2008. *Cobit - 4th Edition (Version 4.1)*, (3 ed.). Rolling Meadows, USA: Information Systems Audit and Control Foundation, IT Governance Institute.

Jobst, A. A. 2007. "It's All in the Data – Consistent Operational Risk Measurement and Regulation," *Journal of Financial Regulation and Compliance* (15:4), pp. 423-449.

Johnson, E. C. 2006. "Security Awareness: Switch to a Better Programme," *Network Security* (2006:2), pp. 15-18.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., and Van Bruggen, D. 2014. "An Exploratory Investigation of Message-Person Congruence in Information Security Awareness Campaigns," *Computers & Security* (43), pp. 64-76.

Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. 2013. "One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions," in: *PACIS 2013*.

Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. "Information Systems Security Policies: A Contextual Perspective," *Computers & Security* (24), pp. 246-260.

Kolkowska, E. 2011. "Security Subcultures in an Organization - Exploring Value Conflicts," *The 19th European Conference on Information systems* Helsinki, p. Paper 237.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. 2014. "Information Security Awareness and Behavior: A Theory-Based Literature Review," *Management Research Review* (37:12), pp. 1049-1092.

Marsden, R., and Salmon, J. 2015. "Barclays Security Scandal: Police Find Stolen Usb Stick Holding Personal Data of 13,000 Customers, Including National Insurance Numbers and Passport Details," in: *Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-3173866/Security-breach-shambles-Barclays-Fraudsters-personal-financial-details-13-000-customers-seven-years.html [accessed 24.07.2015].

Maruna, S., and Copes, H. 2004. "What Have We Learned from Five Decades of Neutralization Research?," *Crime and Justice* (32), pp. 221-320.

Mayring, P. 2003. *Qualitative Inhaltsanalyse: Grundlagen Und Techniken*, (8. ed.). Weinheim: Beltz.

Merhi, M. I., and Midha, V. 2012. "The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study," *Proceedings of the International Conference on Information Systems (ICIS)*, Orlando: Association for Information Systems, pp. 1-11.

Meso, P., Ding, Y., and Xu, S. 2013. "Applying Protection Motivation Theory to Information Security Training for College Students," *Journal of Information Privacy & Security* (9:1), pp. 47-67.

Novotny, A., Bernroider, E. W. N., and Koch, S. 2012. "Dimensions and Operationalisations of It Governance: A Literature Review and Meta-Case Study," *International Conference on Information Resource Management*, R. Brandtweiner and L. Janczewski (eds.), Vienna: The University of Aukland and WU Vienna, pp. 1-12.

ORX, O. R. e. 2014. "Orx Report on Operational Risk Loss Data."

Padayachee, K. 2012. "Taxonomy of Compliant Information Security Behavior," *Computers & Security* (31:5), pp. 673-680.

Pahnila, S., Karjalainen, M., and Siponen, M. 2013. "Information Security Behavior: Towards Multi-Stage Models," *Pacific Asia Conference on Information Systems (PACIS)*, Jeju Island (Korea).

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & Management*).

PricewaterhouseCoopers. 2014. "Information Security Breaches Survey," in: *The Department for Business, Innovation and Skills*. London: Infosecurity Europe, Price Waterhouse Coopers.

Quagliata, K. 2011. "Impact of Security Awareness Training Components on Perceived Security Effectiveness," *ISACA Journal* (4).

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The journal of psychology* (91:1), pp. 93-114.

Rogers, R. W., Cacioppo, J. T., and Petty, R. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology: A Sourcebook*. pp. 153-177.

Sarstedt, M., Ringle, C. M., and Hair, J. F. 2011. "Pls-Sem: Indeed a Silver Bullet," *The Journal of Marketing Theory and Practice* (19:2), pp. 139-152.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. 2009. "The Impact of Information Richness on Information Security Awareness Training Effectiveness," *Computers & Education* (52:1), pp. 92-100.

Silic, M., and Back, A. 2014. "Information Security: Critical Review and Future Directions for Research," *Information Management & Computer Security* (22:3), pp. 279 - 308.

Siponen, M. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.

Siponen, M., Adam Mahmood, M., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies an Empirical Investigation," *IEEE Computer* (43:2), pp. 64-71.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Sommestad, T., and Hallberg, J. 2013. "A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance," *International Information Security and Privacy Conference*: Springer Verlag Berlin Heidelberg.

Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies," *Information & Management* (48:7), pp. 296-302.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24:2), pp. 124-133.

Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Association* (22:6), pp. 664-670.

Thomson, M. E., and von Solms, R. 1998. "Information Security Awareness: Educating the Users Effectively," *Information Management & Computer Security* (6:4), pp. 167-173.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2013. "Managing the Introduction of Information Security Awareness Programmes in Organisations," *European Journal of Information Systems*).

Van Niekerk, J. F., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:4), pp. 476-486.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conductiong Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.

Warkentin, M., Straub, D., and Malimage, K. 2012. "Featured Talk: Measuring Secure Behavior: A Research Commentary," in: *Annual Symposium of Information Assurance & Secure Knowledge Management*. Albany, NY.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Wilson, M., and Hash, J. 2003. "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology (NIST) Special Publication 800-50, Gaithersburg.

Yin, R. K. 2009. *Case Study Research*. Sage Publications.

Appendix

List of Articles of the Dissertation

Dissertation Stage	Publication Output
Stage 1: Exploratory Research	Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.
Stage 1: Exploratory Research	Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.
Stage 1: Exploratory Research	Bauer, S., and Bernroider, E. W. N. 2013a. "IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.
Stage 1: Exploratory Research	Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2013. "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.
Stage 2: Single Case Study	Bauer, Stefan, Bernroider, Edward W.N.. „From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization," *The DATA BASE for Advances in IS* (accepted as research article).
Stage 3: Quantitative Research	Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust*, 154-164, Hrsg. Los Angeles
Stage 4: Multiple Case Study	Bauer, Stefan, Chudzikowski, Katharina. 2015. „Mind the Threat! A Qualitative Case Study on Managing Information Security Awareness Programs in Central and Eastern European Banks," In *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Hrsg. Allen Lee, Puerto Rico.
Stage 4: Multiple Case Study	Bauer, Stefan, Chudzikowski, Katharina, Bernroider, Edward. „Prevention is better than Cure! Designing Information Security Awareness Programs to Overcome the Security Digital Divide in CEE Banks" (submitted as research article).

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector

Stefan Bauer
Vienna University of Economics and Business
stefan.bauer@wu.ac.at

Abstract
In the last decade public authorities have put many global and local regulations for financial institutions into practice. Several of these regulations concern operational IT risks of financial institutions. For financial institutions using the Advanced Measurement Approach operational risk is important to calculate their minimum capital requirements. The objective of this paper is to provide a comprehensive literature review concerning operational risks, regulations and financial institutions. 37 scientific articles were analyzed and categorized by Basel II operational risk definition. Research gaps were identified in particular regarding the role of IT to balance of minimum capital requirements, the use of operational risk information systems and the discovery of toxic combinations of privileges within and outside of IT systems and services.

Keywords
Operational Risk, IT-Risk, Regulation, Basel II, SOX, Solvency II, banking sector, insurance sector, financial sector, Literature Review

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

1. Introduction

There has been growing interest in operational risk management. The main reasons for this are that numerous financial institutions reported operational losses and the recent financial crisis (Acharyya 2010, Goldstein et al. 2010). For example, UBS incurred an operational loss due to fraudulent behavior of one of its traders (BBC 2011). Another example displaying the severeness of the turmoil in the financial service industry even better is that, in 2008, 119 banks reported operating losses to the Standards Implementation Group (SIGOR) amounting to a total sum of € 59.6 billion (Basel Committee 2009). As demonstrated by these examples, operational loss events are multifaceted and thus, complex. They range from categories such as internal and external fraud to business interruptions caused by system failure (Goldstein et al. 2011). Given the inherent complexity of these events, operational risk management is a topic of interest for future research.

International public authorities have been implementing a vast amount of regulations to prevent the economy and, especially, the financial sector, from incurring operational losses in the future. In the early 2000s (e.g. Enron, Tyco, WorldCom), the US government passed the Sarbanes Oxley Act (SOX) (United States Congress 2002). The Sarbanes Oxley Act is compulsory for all companies which are listed on a US stock exchange. SOX should have enhanced public confidence in financial reporting, the auditing professions, and financial markets (Forcht & Luthy 2006). The European Parliament has passed a directive similar to SOX, called EUROSOX, which was incorporated by all EU members (The European Parliament and the Council of the European Union 2006). In addition, Basel II was published by the Basel Committee on Banking Supervision (Basel Committee 2006). Since 2007, Basel II has been compulsory for all credit and financial service institutions in the European Union (Moosa 2007). Basel II sets minimum capital requirements for banks (Jobst 2007b). Currently, Basel III is being implemented with an aim to further strengthen the resilience of the banking sector (Härle et al. 2010).

The minimum capital requirements for operational risks are determined through three different measurement approaches, causing variations in the minimum level of capital required (Mikes 2009). Because of the link between operational risk and minimum capital requirements, banks are interested in the reduction, transfer, or elimination of operational risks (Flores et al. 2006). With the Solvency II directive, European insurance companies are going to face a regulation similar to Basel II, because Solvency II also uses operational risks to determine solvency capital requirements (Acharyya & Johnson 2006). Figure 1 gives a summary of several selected regulations and standards. Through this wave of new regulations in the last decade, operational risk management of financial institutions has become more challenging, but at the same time, more important than ever before.

The purpose of this paper is to present an overview of academic literature on the topic of operational IT risk management in financial institutions. For financial institutions the link between operational risk management and minimum capital requirements has received considerable attention (Jobst 2007b). The focus of this paper is the academic literature starting in 2002, because the most important regulations (e.g. SOX, Basel II) were put into practice from this period onwards. A systematic literature review is useful to offer a clear view on operational risk management and regulation. In this paper, I will focus on the information technology aspect of operational risk management, because there is a lack of detailed research on IT operational risk (Goldstein et al. 2011). Because information is the most important asset of financial institutions, information technology becomes necessary for survival (Goldstein et al. 2011).

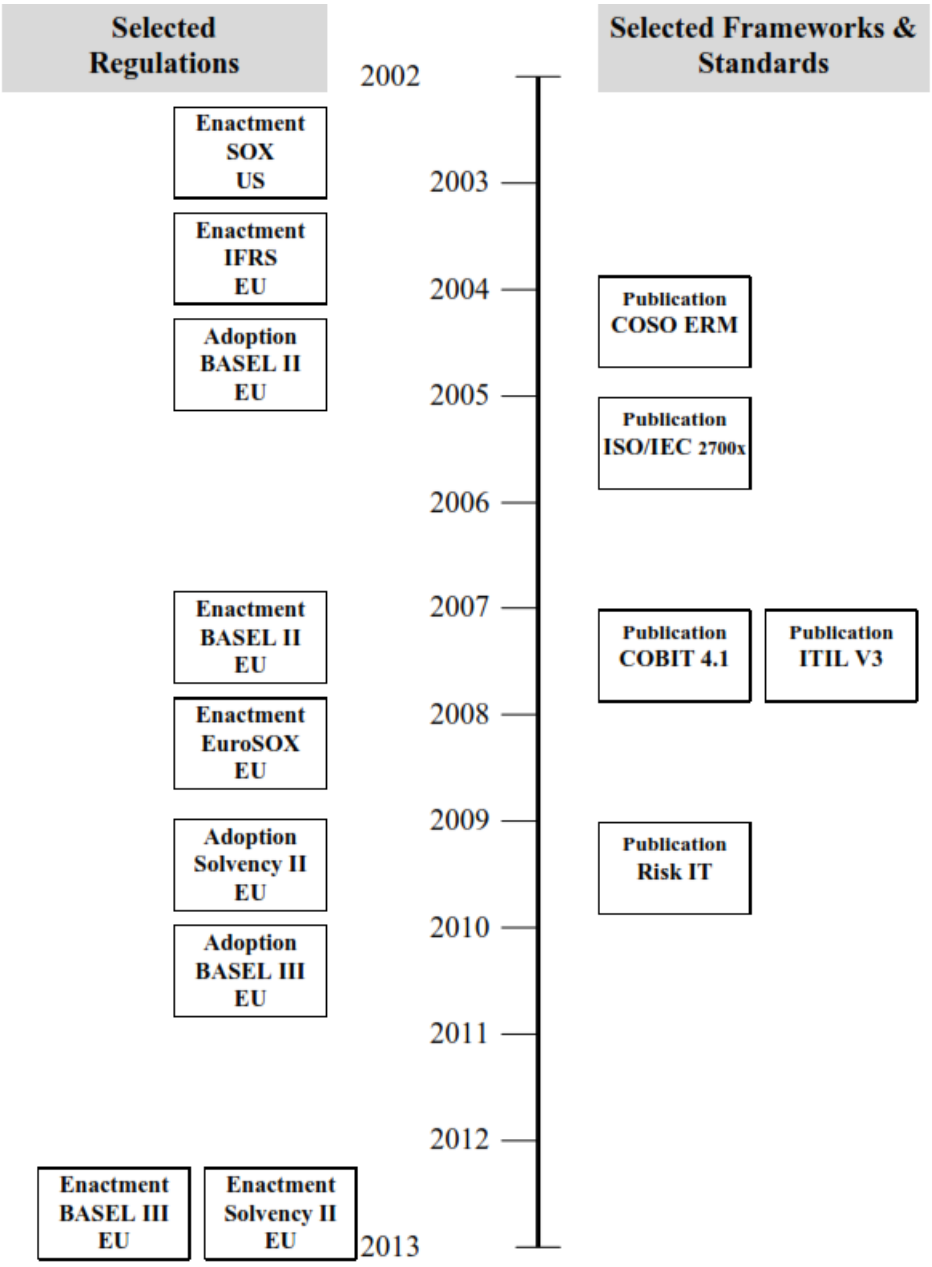


Figure 1: Selected regulations, standards and frameworks and their enactment periods

The paper is divided into five sections. The paper begins by briefly describing the significance of the topic for scientific research and describes methodological aspects. The second section considers definitions and boundaries of current research. In the third section, the methodological framework is discussed. The research process is visualized through Figure 2. In section four, the main concepts are analyzed. The concluding section summaries literature gaps.

2. Theoretical background

Several authors have stated that the academic literature on operational risk in the financial sector is often inconsistent and takes several different views (Acharyya 2010, Moosa 2007). Some authors of the late 90's saw operational risk as the residual that is not faced by credit or market risk (Wahlström 2006). According to Moosa (2007) this approach was too broad and not specific enough. Most of the researched articles for this literature review refer to the Basel II operational risk definition.

In this paper, the term operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (Basel II 2004, p.137). At this point it is important to consider that operational risks have three dimensions. There is the cause, the event, and the consequence (Mossa 2007). The Basel Committee of Banking Supervision classifies operational risk on the event dimension, thus this research also discuss the event taxonomy. The operational risk definition from Basel II excludes strategic risks. Acharyya (2010) mentioned that this exclusion doesn't reflect reality. The author studied the relationship between strategic risk in the enterprise risk management framework and operational risk in financial institutions. He found that strategic management influences many areas where operational risks occur (Acharyya 2010). Because of this reason, this paper extends the Basel II taxonomy with strategic risk.

So far little attention has been given to information technology aspects of operational risks, which occur in every event type category of Basel II operational risk definition (cf. Goldstein et al. 2011). The term 'IT operational risk' is generally undertsood as "any threat that may lead to the improper modification, destruction, theft, or lack of availability of IT assets" (Straub & Welke 1998, p.442). In this research the term is also used according to Goldstein et al. (2011), who distinguishes between data-related IT operational risk and function-related IT operational risks as follows: "Data-related IT operational risk is any threat to the confidentiality of data assets that can result in the disclosure, misuse, or destruction of these assets. Function-related IT operational risk is any threat to the availability or to the integrity of functional IT assets" (Goldstein et al. 2011, p.610). Thus, this literature review also focuses on the differences between approaches on operational risks in the direction of IS/IT.

The investigated regulations are comprehensive and therefore, this review concentrates on specific sections of the analyzed regulations. Basel II consists of three pillars. The present paper gives attention to the first pillar, and within the first pillar on operational risks, and not on credit or market risks (Flores et al. 2006). Section 404 is for the purpose of this paper the most interesting section of SOX, because this section discusses the effectiveness of internal controls. Internal controls and in series operational risk information systems are of increasing importance in consideration of the Advanced Measurement Approach of Basel II (Koutoupis & Tsamis 2008). The relevant part of Solvency II focuses on new methods for calculating capital requirements and new internal control systems (Bónson et al. 2010). After the definitions and boundaries of the topic, the next step is to explain the research methodology.

3. Methodology

The present paper provides a literature review according to the methodology of Watson and Webster (2002). As can be seen from Figure 2, this study consists of three fundamental parts: research definition, research methodology, and research analysis. The paper starts with the research definition, which is presented in the introduction and in the second section. In the first sections the research area is identified, the research goals are formulated, and the scope is defined. Thereafter, follows the research methodology in section 3. The analyzed papers were selected through a keyword based research in the following academic meta-databases: Web of knowledge (SSCI), ProQuest, IEEE computer society, Science Direct, Springer Journals, Emerald online, ACM Digital Library, and Google scholar. In addition, the journal database of the Journal of the AIS was searched. The used keywords and how they were applied are seen in Figure 2. Not a simple Boolean AND operation was applied. Articles were manually screened for relevance.

The research framework (Figure 2) shows a list of the used keywords. Furthermore, during the research process, the identified papers were used to find new relevant literature following a snowball system. This causes the discovered literature to be quite divers. The criteria for the acceptation of an article were that the articles had to be related to all of the three research interests: banking/insurance sector, regulation (Basel II, SOX, Solvency II) and IT operational risks. The researched papers must have been published between 2002 and 2011. This ten year period seems to be appropriate, because as seen in Figure 1, within this period the most relevant new regulations such as SOX or Basel II were put into practice.

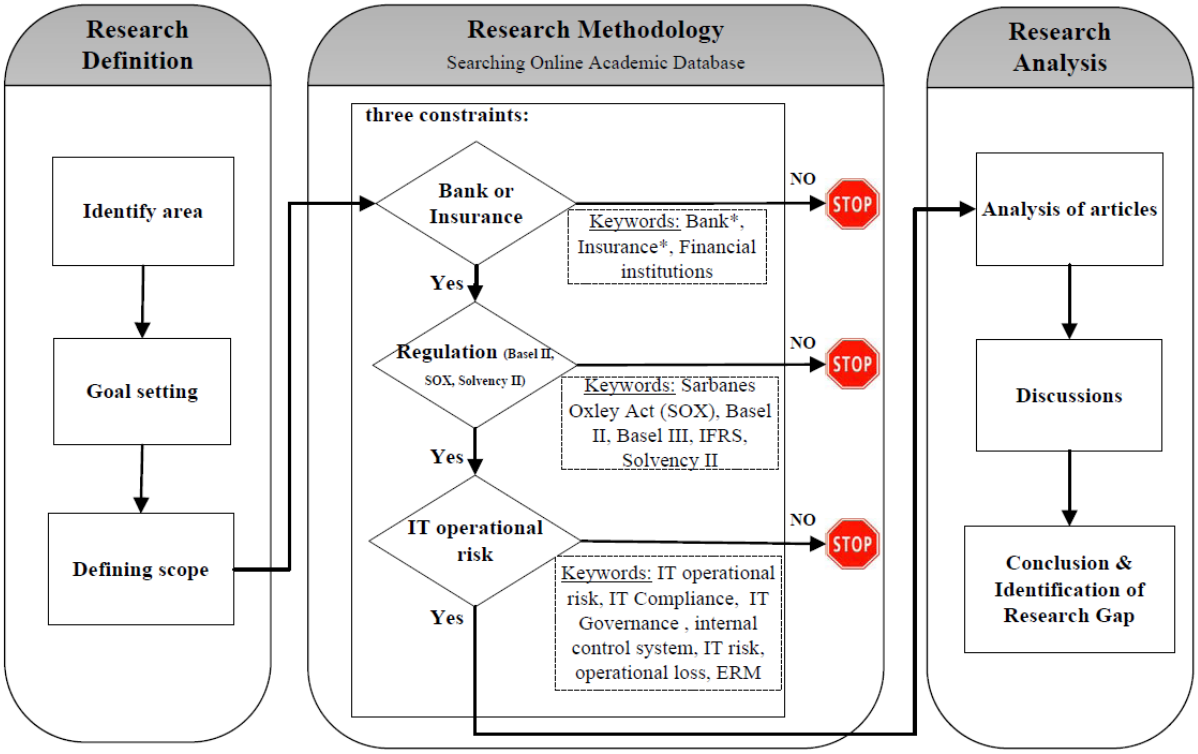


Figure 2: Methodological Framework

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

4. Analysis of the Literature

This chapter presents the analysis of the literature. The first subsection investigates the quality of journals publishing identified articles. In Section 4.2. the frequency of occurrence of regulations and sectors is shown. In the next subchapter the articles are evaluated statistically by frameworks and standards. The methodologies of the researched articles are described in Section 4.4. The main concepts of the articles are characterized in Section 4.5. The subchapters of Section 4.5. investigate the main findings and interesting research areas of the articles. The section is divided into five subchapters and begins by analyzing the articles classified as the holistic view of operational risk, followed by the measurement and reporting approach. The paper goes on with a critical review of articles relating to organizational complexity and risk from people, systems and processes, and strategic risks. Section 4.6. discusses the Basel II Loss Event Type Classification. Finally, the last subchapter looks at the differences between banking and insurance sectors.

Quality of Journals

Altogether this research focuses on 37 scientific articles of different quality. A method to identify the quality of the articles is to categorize them by journal quality. Quality is determined by the 'Academic Journal Quality Guide' (Harvey et al. 2010). The journal quality ranking reaches from one to four stars. One of the researched 37 articles was published in a four stars top journal, and further six articles were issued in three stars journals. Five papers were found in one star journals and eight articles were publshed in journals that were not classified by the ranking. 17 articles are published in conference proceedings of information management related conferences. These results may be interpreted that there is a lack of publications on the research topic in excellent and very good journals.

Classification of Articles by Regulation and Sector

This section deals with the classification of articles by regulation and sector. Figure 3 illustrates the frequency distribution of these articles according to different regulations and sectors.

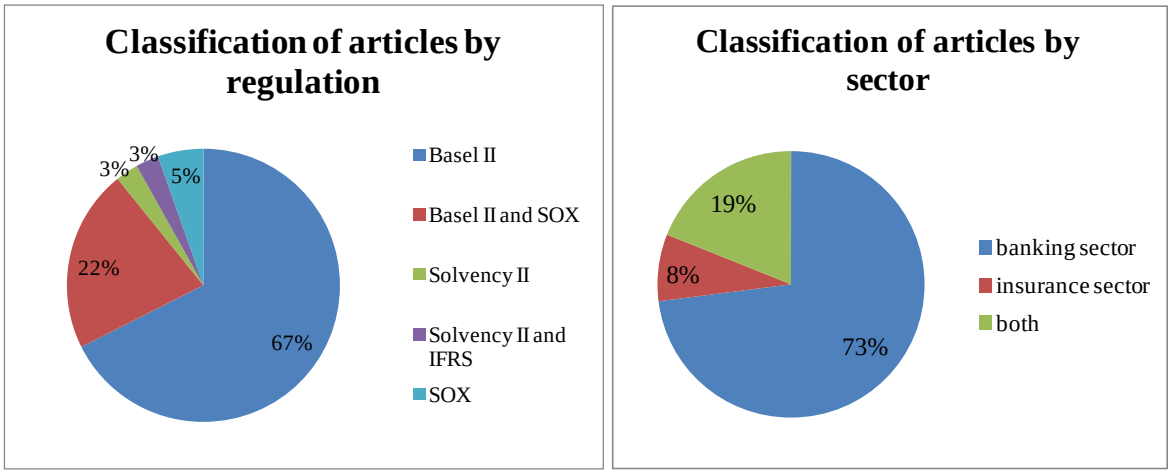


Figure 3 Occurrence of Articles in Sectors, differentiated by Regulations

As can be seen from Figure 3, Basel II appears in 89% of the researched articles. 67% of the articles refer only to Basel II and 22% discuss SOX and Basel II. Exclusive SOX discussions were found in 5% of the articles. There is a lack of literature on Solvency II, as just 6% of articles deal with this regulation. The reason for this result may be that Solvency II is relatively new, because Solvency II was adopted in 2009 and it is going to be enacted in 2013. Another gap of literature regards Basel III, which was not found in academic literature, but in articles of consulting companies. (Härle et al. 2010)

From the data in Figure 3, it can be concluded that most literature deals with the banking sector or the banking and the insurance sector. 73% of the articles refer to the banking sector and 19% to both, the banking and the insurance sector. Only 8% of the articles discuss the insurance sector exclusively. This frequency distribution may also be explained by Solvency II's relatively recent implementation.

Classification of Articles by Frameworks and Standards

There is a substantial amount of research that has discussed standards for risk management (e.g. COSO, Risk IT, ISO 27000, CAS) or government frameworks (e.g. CobiT). Eight articles refer to the COSO risk management framework and five articles mention the CobiT framework. Four articles discuss different ISO standards. Risk IT and ITIL were stated both each three times. Some standards were used only one or two times (e.g. CAS, process reference model). As several articles demonstrate, standards and frameworks are very useful to manage operational risks successfully (Forcht & Luthy 2006, Pardo et al. 2011).

Applied Research Methodologies

Methodologies are indicators to analyze the deepness of research of the underlying topic. Twenty-two of the researched articles are classified as an exploratory or descriptive study. These articles explore or describe their research aims. Furthermore, there are ten case studies and two field studies, which investigated their research topic by one or more cases. Only two of the thirty-seven researched articles are event studies, which rely on real operational risk or operational loss data from OpVar and FIRST databases (Cummins et al. 2006, Goldstein et al. 2011). One article is a multi-method study, containing qualitative and quantitative research. In interpreting these findings, we have to consider that in the financial sector quantitative studies are hard to execute, because operational risks and operational losses are sensitive topics for banks and insurance companies. Previous research has neglected to provide comprehensive quantitative research on this topic.

Basel II Classification

Table 1 provides an overview about the grouping of the investigated literature. The research articles were classified by approaches abstracted from Basel II definition of operational risk, extended by strategic risks. Operational risks can be divided in internal and external loss events. In this review there is no paper which explicitly refers to external loss events, thus there is no section for this loss type.

Article	Holistic	Process	People	Systems	Measure	Strategic
Abdullah et al. (2011)					X	
Acharyya (2010)						X
Acharyya and Johnson (2006)	X					
Atkinson et al. (2006)				X		
Ayerbe et al. (2010)			X			
Bernard et al. (2007)		X				
Bonson et al. (2010)					X	
Cummins et al. (2006)	X					
Dalla Valle and Giudici (2008)					X	
Flores et al. (2006)					X	
Forcht and Luthy (2006)					X	
Gao and Sun (2010)			X			
Gewald and Hinz (2004)		X				
Goldstein et al. (2008)	X					
Goldstein et al. (2011)				X		
Hinz (2005)				X		
Jobst (2007a)					X	
Jobst (2007b)	X					
Koutoupis and Tsamis (2008)					X	
Locher (2005)					X	
Locher et al. (2004)					X	
Longo (2009)	X					
Mikes (2009)						X
Moosa (2007)	X					
Neirotti and Paolucci (2007)				X		
Oh et al. (2007)	X					
Pardo et al. (2011)	X					
Romanovs et al. (2008)				X		
Rotaru et al. (2009)					X	
Sinclair et al. (2008)			X			
Spears and Barki (2010)			X			
Supatgiat et al. (2006)		X				
Svata and Fleischmann (2011)	X					
Wahlström (2004)		X				
Weiß and Winkelmann (2011)		X				
Yang et al. (2010)	X					
Zoet et al. (2009)		X				

Table 1 Articles classified by concepts of Basel II

The next subsections discuss the articles of Table 1 according to the introduced Basel II classifications.

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

Holistic View
Several recent studies have focused on operational risk management in a holistic view (Mossa 2007, Svata & Fleischmann 2010). These articles discuss economic effects or new knowledge about operational risks in general. More sophisticated methods would be required to fully understand the gap between real operational losses and estimated operational risks. This uncertainty leads to a dilemma; choosing between too little or too much capital requirements. A shortage of capital could cause a collapse of the bank and excessive capital could reduce competitiveness and financial leverage (Flores et al. 2006). As Oh et al. (2007) has noted, efficient risk management in financial institutions can arise from reduction in compliance costs or from preventing loss from fraud (Oh et al. 2007).

Operational Risk Measurement Approaches and Operational Risk IS

Basel II (2004) defines in opposite to the old 1988 Basel Capital Accord three measurement approaches for operational risk capital requirements (Jobst 2007a). There is the Basic Indicator Approach, the Standard Approach, and the Advanced Measurement Approach. The Basic Indicator approach and the standard approach are static and easy to measure, because they use fixed percentages of banks' gross income to compute capital charges for operational risk (Abdullah et al. 2011, Flores et al. 2006, Jobst 2007b). Thus, an over- or underestimation of operational risk is likely (Flores et al. 2006). Both approaches are useful for small banks (Dalla Valle & Guidici 2008). Several authors have suggested that the Advanced Measurement Approach could lead to an efficient risk management and reduce capital requirements (Locher 2005, Forcht & Luthy 2006). The Advanced Measurement Approach could be implemented in three different ways: the scenario-based approach, the scorecard approach and the loss distribution approach (Locher et al. 2004). These approaches rely on empirical estimates of operational losses.

The estimation of operational losses is very difficult for financial institutions, because there is a lack of operational loss data (Dalla Valle & Guidici 2008). Because of this, the Advanced Measurement Approach asks for an operational risk information system to identify risks and capital requirements (Flores et al. 2006). Information technology is the key enabler of operational risk management strategies (Oh et al. 2007). The study of Flores et al. (2006) focuses on the benefits of an effective operational risk information system. Such an information system could mitigate risks, thus reduce equity requirements and therefore, the financial institution could be more competitive. There is a trend to the standardization of reporting (Bónson et al. 2010). The Committee of European Banking Supervisors (CEBS) forces a XBRL-based project called COREP-FINREP, which tries to implement banking risks and international accounting regulation (Bónson et al. 2010). As Acharyya & Johnson (2006) has noted, the solution in reporting operational risks is to encourage the employees or business entities to give notice of a loss event so that a database and an information system could be established.

People and organizational complexity
Management culture, organizational structure and the personal opinions of employee's influences operational risks management (Méndez et al. 2010). Sinclair et al. (2008) discovered the organizational complexity and points out toxic combinations of privileges. "A toxic combination is a conflict of system access permissions that allows a user to break the law, violate rules of ethics, damage customers' trust, or even create the appearance of impropriety." (Sinclair et al 2008, p. 167) This problem occurs in the case of promotions, if an employee has access to write checks and afterwards he would be promoted to a position, where he can delete check writing records (Sinclair et al. 2008). Another problem is the risk of over-access, which could be mitigated by giving only the right people access to the information they need for their organizational role. Over-access can cause internal fraud and misuse of data (Sinclair et al. 2008). A source of risk could also be that corporate information is consumed out of the companies, because of the easy access to public networks to remote email, smart phones, laptops and tablets (Sinclair et al. 2008).

Systems and Processes
According to Weiß & Winkelmann (2011), there was no business process modeling language which fulfills the requirements of financial institutions. The authors invented a semantic business process modeling language for banks, which considers different views, like the business objective view, the organizational view, and the resource view. For future research, it is recommended to use the business process modeling language of Weiß & Winkelmann (2011).

Strategic
Acharyya (2010) and Mikes (2009) mentioned that strategy and strategic decisions influence the occurrence of operational risks. Mikes (2009) points out that risk identifiers had no influence on strategy or strategic decisions of the organization. This research direction was discussed in many articles relating to aligning IT and strategy, but for the financial industry there is a lack of literature on this research line.

Basel II Loss Event Type Classification
Several authors investigated the classification of loss event types of Basel II, but only two authors had investigated this classification in detail (Goldstein et al. 2011, Cummins et al. 2006). Goldstein et al. (2011) analyzed data of the FIRST

database and pointed out, that 85% of all loss events are allotted to the categories 'external fraud', 'business disruption and system failure' and 'execution, delivery and process management'. Because of the domination of these three event types, future research should concentrate on them. Further Goldstein et al. (2011) mentioned that future research should focus on function-related IT operational risk events, because functional-related events exert on average a greater negative wealth effect.

Differences between bank and insurance sector
Few authors discuss the differences between banks and insurance companies with different outcomes. For Acharyya (2010) operational risks have had bigger impact on the banking industry than on the insurance industry, because banks face an anytime dynamic payment system in contrast to insurance companies. Otherwise Cummins et al. (2006) found out that if an operational loss occurs, then insurance companies are more affected by a market value reduction than banks. The differences between banking and the insurance sector are discussed poorly in the literature, therefore future research is needed.

5. Conclusion

This research paper identifies areas and issues for further investigation regarding IT risks and regulations of financial institutions. Through a systematic multi-step literature search (Watson & Webster 2002) 37 different articles were identified as being within the scope of this study. These articles were descriptively analyzed according to their focal industry sector (banks or insurance companies), targeted regulation, and control frameworks. In addition, this paper has attempted to classify and discuss the papers according to Basel II guidelines and event loss types. To summarize, the following areas among others seem to warrant more attention related to banks and insurance companies in future work:

- The role of IT to achieve a rational balance of capital requirements (over- or underestimation)
- Design and operationalisation of an effective operational risk information system (Flores et al. 2006)
- Incentives for employees or business entities to disclose weaknesses and loss events (Acharyya & Johnson 2006)?
- More ways to mitigate the rife loss event types 'external fraud', 'business disruption and system failure' and 'execution, delivery and process management' (Goldstein et al. 2011)
- Identification and mitigation of toxic combinations of privileges outside and within IT systems and services (Sinclair et al. 2008)
- Access to corporate information over public networks (Sinclair et al. 2008)

A more systematic analysis of the financial sector of a country or region would be useful to get a realistic picture of specific requirements. According to the identified research methodologies, future research should pay more attention to reliability, e.g., by using more triangulation techniques in case studies, and more comprehensive quantitative research. This seems to be necessary to better understand the substantial risks and their treatment in regard to regulations in the financial sector.

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

References

Abdullah, M., Shahimi, S., Ghafar Ismail, A. (2011) "Operational risk in Islamic banks: examination of issues", *Qualitative Research in Financial Markets*, Vol. 3, No. 2, 2011 pp. 131-151

Acharyya, M. (2010) "The role of operational risk and strategic risk in the enterprise risk management framework of financial services firms", *Int. J. Services Sciences*, Vol. 3, No. 1, pp.79–102.

Acharyya, M. and Johnson, J. (2006) "Investigating the development of enterprise risk management in the insurance industry: an empirical study on four major European insurers." *The Geneva Papers on Risk and Insurance: Issues and Practice*, 55-80.

Atkinson, C., Cuske, C., Dickopp, T. (2006) "Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry", *10th IEEE International Enterprise Distributed Object Computing Conference Workshop (EDOCW'06)*

Basel Committee on Banking Supervision (2006) "International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version." Switzerland: Bank for International Settlements

Basel Committee on Banking Supervision (2009) "Results from the 2008 Loss Data Collection Exercise for Operational Risk" Bank for International Settlements

BBC Business News (2011) "UBS trader Kweku Adoboli charged with fraud", Retrieved 15 November 2011, from http://www.bbc.co.uk/news/business-14950873

Bónson-Ponte, E., Escobar-Rodíguez, T., Flores, F. (2006) "Operational risk information system: a challenge for the banking sector", *Journal of Financial Regulation and Compliance* Vol. 14 No. 4, pp. 383-401

COSO (2004) "Enterprise Risk Management Framework", Retrieved 15 November 2011, from http://www.coso.org

Dalla Valle, L., Guidici, P. (2008) "A Bayesian approach to estimate the marginal loss distributions in operational risk management", *Computational statistics & Data Analysis 52*, pp. 3107-3127

Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., Reinard, D. (2007) "Operational Risk Management in Financial Institutions: Process Assessment in Concordance with Basel II", *Software Process Improvement and Practice* 12, pp.321-330

Forcht, K., Luthy, D. (2006) "Laws and regulations affecting information management and frameworks for assessing compliance", *Information Management & Computer Security* Vol. 14 No. 2.; 2006, pp. 155-166

Gewald, H., and Hinz, D. (2004) "A Framework for Classifying the Operational Risks of Outsourcing - Integrating Risks from Systems, Processes, People and External Events within the Banking Industry", *PACIS 2004 Proceedings. Paper 84.* http://aisel.aisnet.org/pacis2004/84

Goldstein, J.; Chernobai, A.; Benaroch, M. (2011) "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories"; *Journal of the Association for Information Systems*

Goldstein, J. Benaroch, M., Chernobal, A. (2008) "IS-Related Operational Risk: An Exploratory Analysis", *AMCIS 2008 Proceedings, Paper 89.* http://aisel.aisnet.org/amcis2008/89

Harvey, C., Kelly, A., Morris, H., Rowlinson, M. (2010) "Academic Journal Quality Guide", *The Association of Business Schools, Version 4*

Härle, P., Lüders, E., Pepanides, T., Pfetsch, S., Poppensieker, T., Stegemann, U. (2010) "Basel II and European banking: Its impact, how banks might respond, and the challenges of implementation", Mc Kinsey&Company

Hinz, D. (2005) "High Severity Information Technology Risks in Finance", *Proceedings of the 38th Hawaii International Conference on System*

ISO/IEC 27005:2008, Information Security - Security Techniques - Information security risk management.

ISO/IEC, ISO/DIS 31000, Risk Management - Principles and Guidelines on Implementation, Switzerland

IT Governance Institute (2007) "COBIT 4.1." Rolling Meadows: ISACA, 2007

IT Governance Institute (2009) "Risk IT: Framework for Management of IT Related Business Risks." *IT Governance Institute* 2009

Jobst, A., (2007a) "It's all in the data – consistent operational risk measurement and regulation", *Journal of Financial Regulation and compliance* Vol. 15 No. 4, 2007, pp. 423-449

Jobst, A., (2007b) "The treatment of operational risk under the New Basel framework: Critical issues", *Journal of Banking Regulation*, Vol. 8, 4 pp.316-352

Koutoupis, A., Tsamis, A. (2009) "Risk based internal auditing within Greek banks: a case study approach", *Journal of Management and Governance* 13: pp.101-130

Locher, C., Mehlau, J., Wild, O., (2004) "Towards Risk Adjusted controlling of Strategic IS Projects in Banks in the Light of Basel II", *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*

Locher, C. (2005) "Methodologies for Evaluating Information Security Investments – What Basel II can Change in the Financial Industry", *ECIS 2005 Proceedings*. Paper 122 http://aisel.aisnet.org/ecis2005/122

Bauer, S. 2012. "A Literature Review on Operational It Risks and Regulations of Institutions in the Financial Service Sector," *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012)*, Vienna, pp. 1-14.

Longo, E. (2009) "The Knowledge Management Role in Mitigating Operational Risk", *European Conference on Intellectual Capital 2009*

Méndez, C., Camargo; G. and Herrera, A. (2010). "Good Practice Guide for Managing IT Risk in Colombian Banking: Specification by Disciplines", *AMCIS 2010 Proceedings*. Paper 511. http://aisel.aisnet.org/amcis2010/511

Mikes, A. (2009) "Risk management and calculative cultures", *Management Accounting Research 20*, pp. 18-40

Moosa, I. (2007) "Operational Risk: A Survey", *Financial Markets, Institutions & Instruments*, Vol. 16, No. 4, pp. 167-200

Neirotti, P., Paolucci, E. (2007) "Assessing the strategic value of Information Technology:An analysis on the insurance sector", *Information & Management* 44 (2007) pp. 568-582

Oh, L.; Phua, T.; and Teo, H. (2007) "A Conceptual Model for IT-Enabled Enterprise Risk Management in Financial Organisations", *ECIS 2007 Proceedings. Paper 191*. http://aisel.aisnet.org/ecis2007/191

Pardo, C., Pino, F., García, F., Piattini, M., Baldassarre, M., Lemus, S. (2011) "Homogenization, Comparison and Integration: A Haromonizing Strategy for the Unification of Multi-models in the Banking Sector", *PROFES 2011, LNCS 6759*, pp. 59-72

Rotaru, K.; Wilkin, C.; Ceglowski, A.; and Churilov, L. (2009) "Towards operational risk-aware information systems: A critical realist perspective", *ECIS 2009 Proceedings*. Paper 106. http://aisel.aisnet.org/ecis2009/106

Sinclair, S., Smith, S., Trudeau, S., Johnson, E., Portera, A. (2008) "Information Risk in Financial Institutions: Field Study and Research Roadmap", *FinanceCom 2007, Montreal, Canada Lecture Notes in Business Information Processing 4* Springer 2008

Straub, D., Welke, R. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision-Making", *MIS Quarterly* (22: 4, December), pp. 441-469

Svatá, V., Fleischmann, M. (2011) "IS/IT Risk Management in banking industry", *Acta oeconomica pragensia* 19, 3/2011, ISSN 0572-3043

Supatgiat, C., Kenyon, C., Heusler, L. (2006) "Cause-to-effect operational-risk quantification and management", *Risk Management* 8, pp. 16-42

The European Parliament and the Council of the European Union (2006) "Directive 2006/43/EC of the European Parliament and of the Council," Retrieved 15 November 2011, from http://eur-lex.europa.eu

United States Congress (2002) "The Sarbanes-Oxley Act of 2002", Retrieved 15 November 2011, from http://www.law.uc.edu/CCL/SOact/soact.pdf

Watson, R., Webster, J. (2002) "Analyzing the past to prepare for the Future: Writing a Literature Review", *MIS Quarterly* Vol. 26 No. 2, pp. xiii-xxiii/June 2002

Weiß, B. and Winkelmann, A. (2011) „Developing a Process-Oriented Notation for Modeling Operational Risks – A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry", Proceedings of the 44th Hawaii International Conference on System Sciences

Yang, F., LE, Q., Shao, P., Li, D. (2010) "Commentary on the Supervision of Foreign Banking IT Risks", *International Conference on E-Business and E-Government*

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

IT operational risk management practices in Austrian banks: Preliminary results from exploratory case studies

Stefan Bauer
Vienna University of Economics and Business
Stefan.Bauer@wu.ac.at

Edward W. N. Bernroider
Vienna University of Economics and Business
Edward.Bernroider@wu.ac.at

ABSTRACT

The aim of this research is to discover practical insights and suitable methods to effectively manage IT operational risk in Austrian banking companies. We applied an exploratory case study approach and data were conducted using semi-structured face-to-face interviews with senior risk managers. The findings further improve our understanding of how operational risk departments are structured, how employee awareness of IT operational risk loss events is fostered, and the use of operational risk measurement approaches. Moreover, we shed light on practical implementation issues of internal controls in the business and IT processes.

KEY WORDS

IT Operational Risk, Internal Control, Minimum Capital Requirements, IT Risk Culture, Regulation, Basel II, Security Awareness, Advanced Measurement Approach, Financial Institutions.

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Introduction

The flood of new regulation in the last decade and high impact operational loss events increase interest in operation risk management in banking companies (Bauer, 2012). Recent IT operational loss events such as information security breaches or software update failures in banks from all over the world substantiate the problematic situation (Goldstein, Chernobai, & Benaroch, 2011). The recent loss event of an estimated £100 million of the Royal Bank of Scotland in June 2012 due to a software update failure is further evidence for the significance of IT risks (Treanor, 2012). Moreover, banking companies are forced to be complaint to the Basel II regulation which obligates the banking companies to manage operational risks (Basel Committee on Banking Supervision, 2004a; Luthy & Forcht, 2006). Banking companies face several problems with the management of operational risks, especially in connection with IT (Oh, Phua, & Teo, 2007).

As major IT related operational loss events demonstrate, the operational continuity of banking services are threatened by IT problems and banks need to enforce risk management to mitigate these loss events (Oh et al., 2007). For banks, IT is a critical success factor for their daily business and for their projects (Svatá & Fleischmann, 2011). The ever-increasing IT complexity exposes the banking organization to a range of vulnerabilities and a wide spectrum of threats. Over all industries, the banking and financial services sector has the highest actual IT budget as percent of revenue (6.0%) in 2010 (Potter, Smith, Guevara, Hall, & Stegman, 2011).

Efficient and effective IT operational risk management is a constituent element of IT governance (Novotny, Bernroider, & Koch, 2012) and essential for banks not only due to their IT intensive business, but also to balance minimum capital requirements and further capital buffers. The more minimum capital is requirement, the less money banks can use for generating profits (Jobst, 2007a). Given an effective operational risk management, banks have to put back less capital to safeguard their organization and comply with Basel regulations.

The aim of this article is to discover effective and efficient IT operational risk management practices of banking companies in Austria. The motivation for this article resulted from the perceived gap in the literature concerning current practices in IT operational risk management in the midst of the current financial sector crises. The underlying research explores practical problems of IT operational risk management and identifies fields for further research. An exploratory case study approach was used to explore the research topic (Benbasat, Goldstein, & Mead, 1987a). Several semi structured face-to-face interviews in Austrian banks were conducted to answer the research questions. Because of the exploratory nature of this paper, new areas of interest were detected and analyzed through the research process. Our findings highlight current practice about building awareness of the employees regarding IT risks, establishing effective internal controls for IT operational loss events and IT operational risk management in general.

This paper has been divided into six sections. The paper begins by briefly describing the purpose of the underlying research. Section two then moves on to consider the literature review and the theoretical background. Section three offers the research method and methodology. Section four provides an aggregation of the results. Section 5 goes on to discuss the results in the context of the research questions. In the concluding section, we also clarify limitations of the research and offer links for further research.

Literature Review and Research Motivation

The underlying research paper focuses on practical insights and effective methods to manage IT operational risk. This chapter deals with structural and measurement issues of operational risk, IT operational risk awareness of employees, IT risk management frameworks and with the research objectives. The literature review should explain important terms and concepts and conduct to the research questions.

Structural and measurement issues

Operational risk is defined by the Basel Committee as, “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk“ (Basel Committee on Banking Supervision, 2004b). The Basel Committee (2004) defined seven different loss types. Each of these loss types could have an influence on the function of IT assets or on data, hence each loss type is important for IT operational risk (Goldstein et al., 2011). Goldstein at al. define IT operational risk as "any threat to the integrity, confidentiality, or availability of data assets or IT assets that create, process, transport and store data” (Goldstein et al., 2011). IT operational risks are managed in a cause-effect relationship and they are strongly interdependent with other risks (Supatgiat, Kenyon, & Heusler, 2006).

There are three different possibilities to calculate the minimum capital requirements for operational risk: the Basic Indicator Approach, the Standardized Approach and the Advanced Measurement Approach (Jobst, 2007b; Wahlström, 2006). In 2011 the consulting firm Deloitte asked 131 financial companies worldwide concerning their operational risk management approach (Hida, 2011). Only 15% of the financial service companies worldwide use the Advanced Measurement Approach (AMA) to calculate the minimum capital requirements for operational risk. 40% of the financial service companies use the Standardized Approach (SA) and 45% still calculate their requirements through the Basic Indicator Approach (BIA) (Hida, 2011). The selection of the measurement approach impacts the reporting of IT operational risk, because the AMA requires the banks to collect internal loss data on a high level (Jobst, 2007b). In this

context, incentives for employees or business entities to disclose weaknesses and loss events are an interesting and prospective topic for banks (Acharyya & Johnson, 2006).
A recent literature review gives an overview of current work about operational risk in banking companies (Benaroch, Chernobai, & Goldstein, 2012; Goldstein et al., 2011). Banks share their loss data with other banks in external databases. The Operational Riskdata eXchange Association (ORX) database collects data from 62 banking groups worldwide and they reported 27,053 individual loss events with a total gross loss of € 9,110 billion in the year 2009 (ORX Association, 2012).

IT Operational risk awareness

At this point it is appropriate to consider the importance and influence of the Basel II regulation for the IT risk culture of banking companies (Jahner & Krcmar, 2005). If banking companies are Basel II complaint, they have to build awareness of their employees concerning IT operational risks (Basel Committee on Banking Supervision, 2004b). The generic nature of the Basel II regulation in this point is a problem for banking companies, because they have only little guidance on the practical implementation of awareness building actions and therefore they are free to select methods (Fox et al., 2011). Hence, it seems important to discover different awareness building practices in banking companies.
Banking companies have to complaint with Basel II and soon with Basel III, and therefore they need to implement internal controls to monitor key risks (IT Governance Institute, 2007). The Institute of Operational Risk define indicators as "metrics used to monitor identified risk exposures over time" (Institute of Operational Risk, 2010). Internal control helps organizations that they reach their compliance goals (IT Governance Institute, 2007). Banks often implement internal controls through key performance or risk indicators in their processes and they can use software tools to monitor the indicators (Wiesche, Berwing, Schermann, & Krcmar, 2011). Further there is the possibility that incentive schemes motivate employees to report IT operational risk events in time and in a good quality (Lin, Guan, & Fang, 2010; Moynihan & Wells, 2010). Banking companies use key risk indicators extracted from the CobiT framework to monitor IT risks (Benaroch & Chernobai, 2012; IT Governance Institute, 2007).

IT Risk management frameworks

Banks can revert to use best practice control frameworks to satisfy auditors, IT managers and consultants and manage the IT related risks in the organization. One well established control framework is the Control Objectives for IT and related Technology (CobiT) framework (ISACA 2008) which is extensively used to control IT related strategies and operations and to support legal compliance with regulative requirements such as those from the Sarbanes Oxley Act or Basel 2 (Hardy, 2006; Kordel, 2004). While the CobiT framework seems to be widely used in practice, academic validity and internal consistency research on CobiT elements is only emerging (Bernroider & Ivanov, 2011; Tuttle & Vandervelde, 2007).

Research Objectives

The above discussion has shown that failure to account for operational risk management has adverse legal and business related implications for banking companies, especially in the light of new upcoming regulations due to the current financial crisis. Furthermore, the significant role of IT in such organizations has been repeatedly identified as source of operational loss events. In accordance with the above key areas, we now define three research questions:

1. How do large Austrian banks define, structure and measure operational risks with a view on Basel II/III approaches (a), loss event databases (b), operational risk domains (c)?
2. How do large Austrian banks build awareness of IT operational risk events among their employees?
3. Which frameworks do Austrian banks use to support the design and implementation of their internal IT control systems?

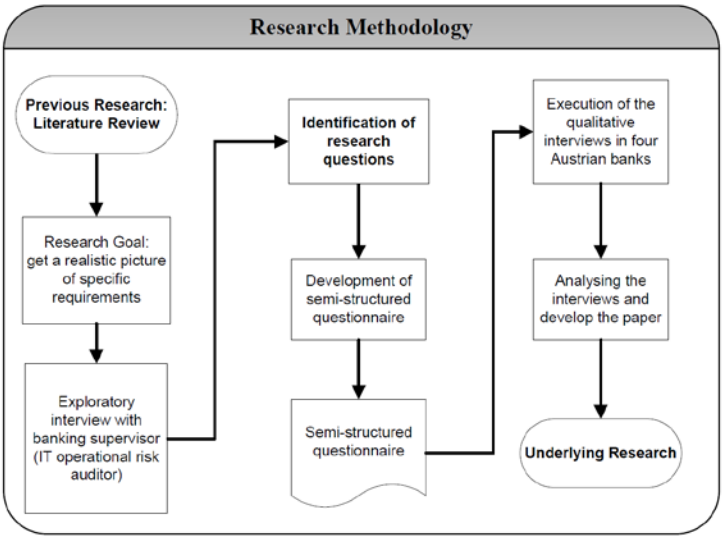
The next section describes how we attempted to answer these questions.

Research Methodology

A case study approach was used to explore the research topic (Benbasat, Goldstein, & Mead, 1987b). Qualitative Interviews were conducted to investigate the research questions regarding IT operational risk management in Austrian banks. The authors carried out an information-oriented selection of the cases (Flyvbjerg, 2011). Figure 1 describes the whole research process.

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Figure 4 Flow diagram of the Research Methodology



At first, an exploratory interview with a banking auditor was carried out to determine which topics and questions could be of practical interest. The outcome of this interview was, that only several big banks in Austria manage IT operational risk professionally. The medium and small banks do not have IT operational risk departments. Therefore the authors selected respondents through the snowball technique and through online social network search. Two respondents were found through the online social networks Xing and LinkedIn. Data were gathered in the period from August to October 2012. Table 1 indicates the position of the employees, the interview types and dates. The interviewer prepared himself by reading the annual report of the banking company before the interview. As a result of this preparation, the semi-structured interviews were individualized depending on the operational risk management conducted in the respective banking company.

Table 1: Interview statistics (exploratory research stage)

Case	Position of interviewee	Type	Dates	Min
1	Head of Operational Risk Management	Face-to-Face Interview	3/9/12	60
2	Operational Risk and Risk Integration (Head)	Face-to-Face Interview	7/9/012	60
3	Head of Group Operational Risk	Face-to-Face Interview	19/9/12	45
4	Head of Group OpRisk Control	Face-to-Face Interview	5/10/12	45

Discussion of Main Results

Table 2 offers an overview of the main outcomes of the interviews structured along our research questions. Based on this overview we subsequently discuss each research question.

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Table 2: Main results from four Austrian large banks along research questions

Qu.	Area	Case 1	Case 2	Case 3	Case 4
1a	Degree of centralization	Central OpRisk departments divided into qualitative and quantitative units, DORMs in single business units			
	ORM approach (Basel II)	SA	AMA	AMA	SA
1b	Internal loss event database in use	Yes	Yes	Yes	Yes
	External loss event database in use	ORX	ORX	ORX	No
1c	Reported OpRisk domains	1. External fraud	1. Execution, delivery and process management;	1. Execution, delivery and process management	1. External fraud
		2. Clients, products and business practices	2. Clients, products and business practices	2. External fraud	2. Internal fraud
2	Main methods for awareness building	E-Learning for all and in-house workshops for DORMs			In-house training, meetings, risk maps
	Incentives for OpRisk event reporting	Monetary rewards	Punishment (if not reported)	No rewards	No rewards
3	IT risk frameworks in use	Modified COSO, COBIT	COSO, COBIT	COSO, COBIT	COSO, COBIT
	Minimum capital requirements §22 (BWG, 2011)	€ 792 million	€ 951 million	€ 897 million	€ 144 million
	Impact of Basel III on OpRisk management	Unknown	Small impact seen	Small impact seen	Unknown

DORMs: Decentralized Operational Risk Managers
ORX: Operational Riskdata eXchange Association
BWG: Bankwesengesetz
COBIT: Control Objectives for Information and Related Technology
COSO: Committee of Sponsoring Organizations of the Treadway Commission
OpRisk: Operational Risk

Structural and measurement issues (Question 1)

First of all (Q1), Austrian banks define and interpret the nature of operational risk in almost the same manner as the Basel Committee (2004). This definition is acknowledged due to the obligatory character of Basel II regulation, which will not change with the enactment of Basel III. In a socio-technical view, Austrian banks focus on loss events that can arise from internal processes (including IT processes), people and systems. In terms of structure, all cases manage operational risk centralized on the entire banking group level, but they also installed decentralized operational risk managers (DORMs) in single business units. The central operational risk management departments are divided in qualitative operational risk management and quantitative operational risk management units. The proportion of the economic risk capital is similar in all researched banks. Credit risk is the most important risk type with a share of approximately 80% of the economic risk capital. Operational risk is covered with nearly 10% and is on the same level as market risk. However, two interviewees pointed out that managing operational risk is at present more important than market risk.

In terms of Basel II measurement approaches (Q1a), only two out of the four large banks use the AMA. One interviewee noted that approximately 50% of the ORX participants calculate their minimum capital requirements with the AMA. The respondent also mentioned a tendency among the ORX participants to strive towards the AMA. However, within the AMA there are differences in calculating the minimum capital requirements. The factors are similar but the weights for the factors differ. One respondent mentioned that for the calculation 33% of the data is fetched from their internal loss database, 33% from an external database and 33% from scenarios and indicators. The selection of the measurement method for calculating the minimum capital requirements are of great interest for banking companies. The respondents mentioned advantages as well as disadvantages for using AMA. The advantages reach from reputation gains to improved financial aspects such as the allowance of insurances due to lower minimum capital requirements. Mentioned disadvantages include the outcome. In previous years the gross income of some banks decreased, and as a consequence using AMA instead of the SA results in higher minimum capital requirements. An explanation is that lower levels of gross income per business line impacts the end results in the SA. Another interviewee declared that all banking groups in Austria besides the biggest four are not big enough to implement AMA simply because they cannot accumulate enough loss events to reasonably operate their internal data base.

With regard to loss event processing (Q1b), all four respondents noted that they work with an external and international internal loss events database. The quantitative operational risk management units are responsible for maintaining the internal loss event data base and calculating the minimum capital requirements in all four cases. However, there are also important differences across the cases. Two different loss event collection approaches can be distinguished:

1. *Centralized approach*: Central collection and uploading of operational loss events to an internal database.
2. *Decentralized approach*: Operational loss events are reported bottom-up and directly fed into the internal database by the employees.

Our findings show that banks, which use the AMA, are more likely to report operational risk events centrally. In contrast, banks not using the AMA are more likely to let their employees directly report operational risk events to their internal databases.

In all researched banks the operational risk department works together with the internal audit, compliance, law and insurance department, to manage operational risks effectively. The operational risk controlling unit is separated from operational risk management. Operational risk is for all four researched banks an important area for the future, therefore two of the four banking companies plan to hire staff for operational risk management.

Operational IT risk awareness (Question 2)

In terms of risk awareness management, all four banking companies use their qualitative operational risk management units to foster risk awareness and develop a risk culture in their organization. The regulation Basel II forces the banks to build awareness of their employees concerning operational risk. Therefore the banking companies all apply awareness building approaches, but use different methods. Three have implemented an obligatory e-Learning system to educate their employees. All respondents reported that operational risk trainings for a specific group of employees was implemented. Especially the employees with responsibilities concerning operational risk reporting (e.g. the DORMs) were trained. In all banks risk and control self assessments and risk meeting were conducted. The outcomes of the self assessments and the expert questionnaires are discussed with line management and the results reported to the central operational risk management unit. In the business lines risk meetings were hold from time to time.

Only one bank connects the quality of the reporting of operational risk events with the compensation of the managers. The managers of this bank were compensated on the base of the economic capital, which bases on risk ratios. A ratio could be how much time is needed from the detection to the reporting of operational risk event. This practice in one bank increases transparency, and helps to monitor and control operational risk management.

IT risk management frameworks (Question 3)

Three respondents use the COSO risk management framework. One interviewee criticized that COSO forces banks to think of phantom risk with high frequency and high severity risks. The same interviewee mentioned that such risks do not exist and because of that COSO could misdirect risk management. Previous research has paid attention to this problematic (Mestchian, Makarov, & Mirzai, 2005). The dominance of COBIT as risk management framework was confirmed by the three out of four cases. The maturity levels of the frameworks are also important for the IT operational risk management, because the level of internal control belongs to maturity level of COBIT and ITIL. IT operational risk management is seen as a continuous improvement process.

All four respondents explained that they monitor operational risk through automated internal controls in their business and IT processes. The banking companies have modelled their processes and implemented key risk indicators. One respondent said that they use similar controls as the Institute for Operational Risk (2010) published in their latest article. The following key risk indicators are used (Institute of Operational Risk, 2010):

- Staff turnover: connected to risks such as fraud, staff shortages and process errors
- The number of data capture errors: process errors
- Number of virus or phishing attacks: IT systems failure
- Percentage of staff not completed primary fraud detection training
- Information technology support requests - number outstanding beyond threshold
- Project Management: number of high-risk projects

As described above, one banking company connects incentives for managers to the quality of reporting and managing operational risk events. Similar to the results of the ORX database, the respondents answered that retail banking is the most important area for operational risk management. One interviewee also mentioned that trading is very crucial, because an operational loss event there could have a huge impact. For cases the importance of an economic approach where the costs of a control do not outweigh its benefits was noted. There seems to be a level of tolerable uncertainty for high frequency and low impact events.

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Conclusion and limitations

More sophisticated methods are needed to discover the effectiveness of incentives for managers on the basis of the economic capital. The respondent mentioned that this incentive system works well and that there is a tendency to compensate managers on risk ratios. Other respondents mentioned that they do not think an incentive system regarding operation risk management make sense. Further research should investigate how the quality of reporting operational risk differs between a bank with and a bank without an incentive system.

Additional research would be necessary to assess the risk culture and the awareness concerning operational risk loss events of the employees in the banking companies. The researched banks force an open risk communication. They use different qualitative methods to reach this goal. Awareness could prevent operational loss events and educate the employees concerning the reporting of operational IT loss events. It seems to be logical that the more employees are educated concerning operational risk, the more the quality of the reporting increase.

An interesting research question concerns E-Learning as a tool for awareness building in banking companies. E-Learning is a popular tool and in two banking companies the employees have to pass an exam after the E-Learning program at the beginning of their engagement. Additional research would be necessary to confirm that the employees are really aware concerning operational risk events after successfully passed an E-Learning program. Future research might concentrate on a comparison of the of the cost-benefit ratio of awareness building provisions, like E-Learning, risk meetings, marketing goodies.

Finally, we acknowledge several limitations. First, only big banks in Austria have an operational risk management unit. Hence, the underlying research is only relevant for this group of banks. Future research is going to focus also on medium and small banks. Second, only the senior managers on the top of the hierarchy of operational risk management were interviewed. They have had a good overview knowledge and therefore sufficed for the general aims of this paper. However, only two of them have worked before in a IT department and therefore only two respondents were able to refer to their own working experiences in terms of IT operational risk.

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

References

Book

Basel Committee on Banking Supervision International Convergence of Capital Measurement and Capital Standards (2004).

Flyvbjerg, B. (2011). Case study. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research, 4th Edition* (pp. 301–316).

Hida, E. T. (2011). Global risk management survey. *Deloitte Research*.

Institute of Operational Risk. (2010). *Operational Risk Sound Practice Guidance - Key Risk Indicators* (p. 44).

ISACA. (2008). COBIT - 4th Edition (Version 4.1) (3 ed.). Rolling Meadows, USA: *Information Systems Audit and Control Foundation*, IT Governance Institute.

IT Governance Institute. (2007). *IT Control Objectives for Basel II*.

ORX Association. (2012). *ORX Operational Risk Report*. Retrieved from http://www.orx.org/orx-data

Potter, K., Smith, M., Guevara, J. K., Hall, L., & Stegman, E. (2011). IT Metrics: IT Spending and Staffing Report. *Egham: Gartner*, (January), 1–70.

Journal

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting*, Retrieved from http://www.sciencedirect.com/science/article/pii/S1467089512000164

Benbasat, I., Goldstein, D. K., & Mead, M. (1987a). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987b). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386.

Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, *29*(3), 325–336. doi:10.1016/j.ijproman.2010.03.002

Fox, C., Mcguire, R., Crickette, G., Drobnis, K., Egerdahl, R., Gjerdrum, D., Gofourth, R., et al. (2011). An overview of widely used risk management standards and ruidelines. *Risk and Insurance Management Society*.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, *12*(9), 606–631.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, *11*(1), 55–61. doi:10.1016/j.istr.2005.12.004

Jobst, A. (2007a). The treatment of operational risk under the New Basel framework: Critical issues. *Journal of Banking Regulation*, *8*(4), 316–352. doi:10.1057/palgrave.jbr.2350055

Jobst, A. (2007b). It's all in the data – consistent operational risk measurement and regulation. *Journal of Financial Regulation and Compliance*, *15*(4), 423–449. doi:10.1108/13581980710835272

Kordel, B. L. (2004). IT Governance Hands-on: Using CobiT to Implement IT Governance. *Information Systems Control Journal*, *2*.

Lin, F., Guan, L., & Fang, W. (2010). Critical Factors Affecting the Evaluation of Information Control Systems with the COBIT Framework. *Emerging Markets Finance and Trade*, *46*(1), 42–55. doi:10.2753/REE1540-496X460105

Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*, *14*(2), 155–166. doi:10.1108/09685220610655898

Mestchian, P., Makarov, M., & Mirzai, B. (2005). Operational risk–COSO re-examined. *Journal of Risk Intelligence*, 19–22. Retrieved from http://www.risk-update.com/uploads/tx_bxelibrary/OpRisk-COSO-Mestchian-SAS-Risk-Journal-2005.pdf

Moynihan, D. P., & Wells, S. (2010). Designing Compensation Plans to Manage Today's Risk Environment. *Compensation & Benefits Review*, *43*(1), 17–22. doi:10.1177/0886368710390490

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, *8*(4), 240–263. doi:10.1016/j.accinf.2007.09.001

Wahlström, G. (2006). Worrying but accepting new measurements: the case of Swedish bankers and operational risk. *Critical Perspectives on Accounting*, *17*(4), 493–522. doi:10.1016/j.cpa.2004.08.006

Conference paper or contributed volume

Acharyya, M., & Johnson, J. (2006). Investigating the development of enterprise risk management in the insurance industry: an empirical study of four major European insurers. *Geneva Papers on Risk and Insurance*. Retrieved from https://www.actuaries.org.uk/sites/all/files/documents/pdf/acharyya.pdf

Bauer, S. (2012). A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector. *Conf-IRM 2012* (pp. 1–14).

Benaroch, M., & Chernobai, A. (2012). IT operational risk events as COBIT control failures: A conceptualization and empirical examination. *Information Systems (ILAIS) Conference* (pp. 115–117). Retrieved from http://ilais.openu.ac.il/wp/wp-content/uploads/2012/07/ILAIS-2012-Proceedings.pdf#page=115

Bauer, S., and Bernroider, E. W. N. 2013b. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from Exploratory Case Study," *Proceedings of the International Conference Information Systems 2013 (IADIS)*, M. Nunes (ed.), Lissabon: IADIS Press pp. 30-38.

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. *Americas Conference on Information Systems AMCIS* (pp. 1–11).

Novotny, A., Bernroider, E., & Koch, S. (2012). Dimensions and Operationalisations of IT Governance: A Literature Review and Meta-Case Study. *International Conference on Information Resource Management, Vienna*. Retrieved from http://aisel.aisnet.org/confirm2012/23/

Oh, L., Phua, T., & Teo, H. (2007). A Conceptual Model for IT-Enabled Enterprise Risk Management in Financial Organisations. *European Conference on Information Systems 2007 Proceedings*. Retrieved from http://aisel.aisnet.org/ecis2007/191

Supatgiat, C., Kenyon, C., & Heusler, L. (2006). Cause-To-Effect Operational-Risk Quantification and Management. *Risk Management*, *8*(1), 16–42. doi:10.1057/palgrave.rm.8250001

Svatá, V., & Fleischmann, M. (2011). IS/IT Risk Management in Banking Industry. *Acta oeconomica pragensia*, 42–60. Retrieved from http://econpapers.repec.org/article/prgjnlaop/v_3a2011_3ay_3a2011_3ai_3a3_3aid_3a334_3ap_3a42-60.htm

Wiesche, M., Berwing, C., Schermann, M., & Krcmar, H. (2011). A Pattern-based Approach to Understanding Control Requirements for Information Systems for Governance , Risk and Compliance. *The 23rd International Conference on Advanced Information Systems Engineering - Caise*.

Newspaper Article

Treanor, J. (2012). RBS computer failure to cost bank 100 million pounds. *The Guardian*, pp. 1–12. Retrieved from http://www.guardian.co.uk/business/2012/aug/02/rbs-computer-failure-compensation

Bauer, S., and Bernroider, E. W. N. 2013a. "IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.

How to reduce IT operational risks in a multi-national bank through building employee awareness and the use of internal controls: A preliminary research design

Stefan Bauer
Vienna University of Economics and Business
Stefan.Bauer@wu.ac.at

Edward W. N. Bernroider
Vienna University of Economics and Business
Edward.Bernroider@wu.ac.at

Research in Progress

Abstract
The purpose of this research in progress is to analyse bank employee risk behaviour concerning IT operational risks in Austrian banks. The two-staged empirical study focuses on the role of IT risk culture and internal controls in relation to employee risk behaviour and the effectiveness of different awareness building practices in banking companies in response to international banking regulation. The findings should discover best practices of awareness building methods and guidelines to create a proactive IT risk culture.

Keywords
Key words: IT Operational Risk, IT Risk Culture, Information Security Awareness, Employee Risk Behavior, IT Governance

Bauer, S., and Bernroider, E. W. N. 2013a. "IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.

1. Introduction

Recent regulations such as Basel II forces banking companies to systematically manage risks and in particular operational risks (Basel Committee on Banking Supervision, 2004; Bauer, 2012). Banks have to reserve minimum capital requirements for potential operational loss events. The more minimum capital is required, the less money banks can use for generating profits (Jobst, 2007). Given an effective operational risk management, banks can put back less capital to safeguard their organization and comply with Basel regulations (Luthy & Forcht, 2006). Recent IT operational loss events such as information security breaches or software update failures in banks from all over the world substantiate the problematic situation (Goldstein, Chernobai, & Benaroch, 2011). The objectives of IT operational risk management largely conform with traditional information security goals, which seek to assure availability, confidentiality, and integrity of data and systems (Benaroch & Chernobai, 2012; Goldstein et al., 2011). Efficient and effective IT operational risk management is a constituent element of IT governance (Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny et al. 2012)(Novotny, Bernroider, & Koch, 2012) and a range of IT controls can be implemented, for example, to reduce IT operational risks caused by IT changes (Bernroider & Ivanov, 2011). More attention is required to understand the role of the employee to detect operational weaknesses and loss events early (Bauer, 2012).

Basel II engages banking companies to build awareness concerning operational risk, especially on information technology aspects of operational risk (Pinder, 2006). However, the generic Basel II regulation does not describe how banks can build awareness. As the research team discovered from exploratory interviews in Austrian banks, banking companies use different practices to train their employees in this context. Austrian banks build employees awareness through an obligatory E-Learning program at organizational entry. Moreover, some banks conduct regular risk meetings in their subunits, self assessments and provide marketing goodies such as coffee cups for the employees. Exploratory interviews in Austrian banks have shown that operational risk managers rate the awareness building process as a very important issue in operational risk management. Operational risk managers have limited financial and human resources and hence they are interested to find effective and innovative ways to successfully build awareness of their employee.

The underlying research in progress is structured in two stages. At first, awareness building methods in banking companies in Austria should be discovered through exploratory interviews with operational risk and information security managers, as well as employees, who passed successfully awareness building programs. The goal of the exploratory interviews is to explore best practices and outcomes of their awareness building methods. In the second step, quantitative research is going to empirically test success of innovative methods and existing techniques in subunits of banking companies.

2. Theoretical Background and Research Hypotheses

Information security cannot be achieved through technology alone (Herath & Rao, 2009), hence banking companies management should focus on the social-cultural perspective of information security (Jahner & Krcmar, 2005). The socio-cultural perspective of IT operational risk management deals with the human factor as a possible reason or influence factor for operational loss events (Jahner & Krcmar, 2005; Thomson, Solms, & Louw, 2006). The upcoming research focuses on the improvement of employee risk behaviour. According to the main body of related literature, risk behaviour deals with attitudes towards negative outcomes and policy compliance (ISACA, 2009; Sitkin, Pablo, & Sim, 1992). To improve the risk behaviour of the employees, the organization needs a functioning and active IT risk culture (Da Veiga & Eloff, 2010; Jahner & Krcmar, 2005). Essential for a functioning risk culture is the behaviour towards negative outcomes, because some organizations established learning cultures, where employees learn from their failures. In contrast, some organizations establish an unintended blaming culture, because they punish their employees if their behaviour does not comply with corporate guidelines (ISACA, 2009). Learning theories such as the social learning theory or the organizational learning theory are of great interest for this research as learning from failures seems to be essential to improve risk behaviour of employees (Argyris, 1977; Thomson et al., 2006).

An increased awareness is the most cost-effective control of an organization (Dhillon, 1999). Different methods can be used for awareness building among the employees, which attempt to educate and inform employees about IT operational risks. Some aspects such as media richness should be more important than others to transfer knowledge (Daft & Lengel, 1986). If the employees are aware of the threats, their behaviour concerning IT operational risks should improve. The highest stage of awareness is when the employees have internalized best practice behaviour (Nonaka, 1994). Hence, these considerations lead us to the following preliminary hypothesis.

H1. Types and dimensions of awareness building methods, such as media richness, are related with achieved improvement levels in terms of IT operational risk awareness of the employees.

Bauer, S., and Bernroider, E. W. N. 2013a. "IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.

Our review of literature and empirical work substantiates that risk behaviour of employees can be improved by making them more aware of the purpose and operation of internal controls. In general, employees seem to know that there is an internal control system, but they do not know what exactly is controlled. Greater levels of awareness should lead to improved IT operational risk behaviour and make it more likely to prevent or timely detect IT operational loss events. An effect similar to the well known productivity improvement effect known as Hawthorne effect is expected (Brannigan & Zwerman, 2001). The Hawthorne experiment highlighted that if an employer pays attention to the performance of employees, the likelihood of increased performance levels increases. The same can be expected in the context of IT operational risk prevention, mitigation and reporting. It is expected that a communication campaign concerning internal control system in the organization improve the risk behaviour of the employees.

H2. The more employees know about the internal control system, the better the employee risk behaviour in terms of preventing and detecting IT operational risk events.

3. Research Methodology

The research methodology is displayed below (see Figure 1). Previous research has reviewed the literature and has executed exploratory interviews with operational risk managers in Austrian banks. In stage 1, a case study in a large banking company will be conducted. Unstructured interviews with employees at several levels will be executed to explore the current awareness programs and employee behaviour. Qualitative interviews and observations of work places will be carried out to discover awareness building methods regarding IT operational risk. As (Vroom & Von Solms, 2004) mentioned, behaviour of individual employees concerning information security is difficult to audit and review, but we plan to use innovative methods to analyse the improvement of risk behaviour such as not reactive measurement methods (e.g. experiment reaction of employees on a stimulus like a specific safety message). After sufficient case study data is obtained, we will know the variables that need greater focus and should be included in our survey questionnaire.

For the survey research in stage 2, the survey instrument will be developed based on the findings from the first phase of our research and an extensive literature review. For example, we seek to discover how E-Learning impacts risk awareness and currently seek to implement pre- and post-questionnaires to analyse learning outcome of this awareness building method. The sampling frame will most likely be all employees from specified organizational units. Before administration of a mass survey, we will seek comments on the clarity and accuracy on conceptualization of the variables from a panel of academic and managers. We will also conduct a pilot test of the survey instrument with a small sample of employees to evaluate the validity and reliability of our survey instrument. After modification of the instrument based on comments from the panel and pilot test, we will launch a survey by delivering the finalized survey questionnaire to our sampling frame in proven multi-staged procedure ensuring an acceptable return quota.

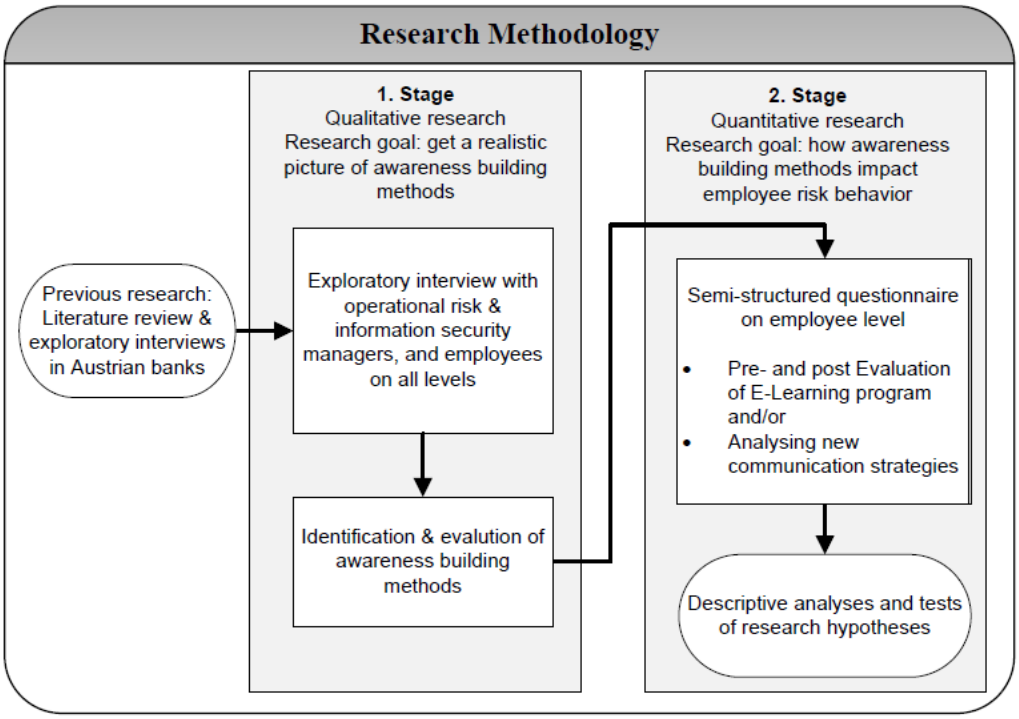


Figure 1: Research model

Bauer, S., and Bernroider, E. W. N. 2013a. "IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems," *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, L. Janczewski (ed.), Natal, pp. 1-4.

4. Conclusion

Banking companies face several problems with management of operational risks, especially in connection with IT and risk cultures. Employee risk behaviour concerning IT operational risk events is driven by awareness of the single employee and IT risk culture in the organization. This research-in-progress seeks to discover best practices of awareness building and empirically tests innovative methods to educate employees to improve their risk behaviour.

References

Argyris, C. (1977). Organizational learning and management information systems. *Accounting, Organizations and Society*, *2*(2), 113–123. Retrieved from http://www.sciencedirect.com/science/article/pii/0361368277900289

Basel Committee on Banking Supervision. (2004). *International Convergence of Capital Measurement and Capital Standards*.

Bauer, S. (2012). A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector. *International Conference on Information Resource Management, Vienna. The University of Aukland and WU Vienna* (pp. 1–14). Retrieved from http://aisel.aisnet.org/confirm2012/58/

Benaroch, M., & Chernobai, A. (2012). IT operational risk events as COBIT control failures: A conceptualization and empirical examination. *Information Systems (ILAIS) Conference* (pp. 115–117). Retrieved from http://ilais.openu.ac.il/wp/wp-content/uploads/2012/07/ILAIS-2012-Proceedings.pdf#page=115

Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, *29*(3), 325–336. doi:10.1016/j.ijproman.2010.03.002

Brannigan, A., & Zwerman, W. (2001). The real "Hawthorne effect". *Society*, 55–60. Retrieved from http://www.springerlink.com/index/T845NT54RQR0WAM3.pdf

Da Veiga, a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. doi:10.1016/j.cose.2009.09.002

Daft, R., & Lengel, R. (1986). Organizational information requirements, media richness and structural design. *Management science*, *32*(5), 554–571. Retrieved from http://mansci.journal.informs.org/content/32/5/554.short

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, (1999). Retrieved from http://www.emeraldinsight.com/journals.htm?articleid=862746&show=abstract

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, *12*(9), 606–631.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi:10.1057/ejis.2009.6

ISACA. (2009). *The Risk IT Framework*. (Information Systems Audit and Control Association, Ed.). Retrieved from http://books.google.com/books?hl=en&lr=&id=tG7VMihmwtsC&oi=fnd&pg=PA7&dq=The+Risk+IT+Framework&ots=TGtaQV5Mxp&sig=VWqP3yBMOzR9UZDJBNoz-rVnFdw

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. *Americas Conference on Information Systems AMCIS* (pp. 1–11).

Jobst, A. (2007). The treatment of operational risk under the New Basel framework: Critical issues. *Journal of Banking Regulation*, *8*(4), 316–352. doi:10.1057/palgrave.jbr.2350055

Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*, *14*(2), 155–166. doi:10.1108/09685220610655898

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization science*, *5*(1), 14–37. Retrieved from http://orgsci.highwire.org/content/5/1/14.short

Novotny, A., Bernroider, E., & Koch, S. (2012). Dimensions and Operationalisations of IT Governance: A Literature Review and Meta-Case Study. *International Conference on Information Resource Management, Vienna*. The University of Aukland and WU Vienna. Retrieved from http://aisel.aisnet.org/confirm2012/23/

Pinder, P. (2006). Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II). *Information Security Technical Report*, *11*(1), 32–38. doi:10.1016/j.istr.2005.12.003

Sitkin, S., Pablo, A., & Sim, B. (1992). Reconceptualizing the determinants of risk behavior. *Academy of management review*, *17*(1), 9–38. Retrieved from http://www.jstor.org/stable/10.2307/258646

Thomson, K., Solms, R. Von, & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, (October), 49–50. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372306704304

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. doi:10.1016/j.cose.2004.01.012

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2013. "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study

Stefan Bauer
Vienna University of Economics and Business
Stefan.Bauer@wu.ac.at

Edward W. N. Bernroider
Vienna University of Economics and Business
Edward.Bernroider@wu.ac.at

Katharina Chudzikowski
University of Bath, School of Management
K.Chudzikowski@bath.ac.uk

Abstract
The purpose of this research is to analyze information security awareness (ISA) programs and the measurement of ISA behavior in banking organizations. The underlying paper summarizes the qualitative and exploratory part of our two-staged mixed methods research on the improvement of employee security behavior concerning IT operational risks. IT operational loss events are often caused by undesirable security behavior of employees concerning information technology. Organizations conduct ISA programs to build employees' security awareness concerning information technology to prevent IT operational loss events. Ten semi-structured qualitative expert interviews were carried out to explore potentials for improvement of ISA programs. Our findings focus on the character of ISA delivery methods and the implemented controls for these methods. Further research should shed light on the effectiveness of experimental and proactive ISA controlling. The outcome provides input for practice in the area of ISA building in the financial sector.

Keywords: Information Security Awareness, Employee Security Behavior, IT Operational Risk, IT Risk Culture, Basel II

1. INTRODUCTION

Information technology (IT) is essential for the operational business of banking companies. Operational loss events can be caused by external (e.g. hackers, social engineers) or internal (e.g. fraud, unintentional security violations) reasons. Noncompliant behavior of employees can enable operational loss events through the use of IT and since Basel II was enacted, banks have to manage operational risk and build minimum capital reserves for IT operational risks (Bauer and Bernroider 2013b). IT operational risk is defined as "any threat to the integrity, confidentiality, or availability of data assets or IT assets that create, process, transport and store data" (Goldstein et al. 2011). As the definition show, the objectives of IT operational risk management conform with traditional information security goals, which seek to assure availability, confidentiality, and integrity of data and systems.

Banks try to protect themselves with technical solutions, like data leak prevention software, but previous scientific research has found out, that technical solutions alone cannot protect an organization from loss events, because employees intentionally or unintentionally bypass existing engineered barriers (Chang and Yeh 2006). One of the biggest threats concerning information security is that most employees do not care about and are not interested in information security (Furnell and Thomson 2009). To identify potentials for improving employee behavior concerning IT operational risks, the underlying research discovers how banking companies currently build and measure information security awareness (ISA) of their employees.

Desirable employee behavior concerning information security can be stated in the information security policy (ISP) of an organization. The ISP should preferably contain the prescribed behavior concerning IT topics like password security, e-mail attachments and internet usage. ISA programs are developed to bring the rules and practices, which can be stated in the ISP, in minds of the employees (Shaw et al. 2009). We assume that some ISA delivery methods are more effective to build ISA of employees than others. Therefore we evaluate real world practices and deduce innovative methods to build ISA.

The paper is divided into five sections. After this short introduction, section 2 explains the theoretical background of the research constructs and postulate research questions. Section 3 goes on to discuss methodological issues of the research in progress paper. In Section 4 preliminary results from the first research stage are presented and section 5 provides a conclusion and a forecast.

2. THEORETICAL FOUNDATION AND RESEARCH

2.1. Taxonomy of End User Behavior

The underlying research considers employees as enablers of IT operational loss events. Desirable behavior of employees is categorized in security assurance behavior (SAB) and security compliance behavior (SCB), while undesirable behavior can be characterized in security risk-taking behavior (SRB) and security damaging behavior (SDB) (Guo 2013). Previous research discovered the motive and expertise of the employee as important factors (Guo 2013; Stanton et al. 2005). Table 1 provides definitions, examples and motives for the above introduced security behavior types.

Table 2 Taxonomy of security behavior according to (Guo 2013)

	Security assurance behavior (SAB)	Security compliant behavior (SCB)	Security risk-taking behavior (SRB)	Security damaging behavior (SDB)
Definition	Active behaviors by an individual who has clear motive to protect the organization's IS	Behaviors that are in line with organizational security policies	Behavior that my put the organization's IS at risk	Behaviors that will cause direct damage to the organization's IS
Examples	Take precaution; report incidents	Refrain from prohibited behavior	Password write-down; copy sensitive data to mobile devices	Crack password; data theft
Motive (from the security perspective)	Beneficial	Neutral	Neutral	Malicious

Every security behavior type from (Guo 2013) could lead to operational loss events, as shown by the examples in table 1 and by (Goldstein et al. 2011) with real world examples from FIRST loss database. Employees often open doors for external attacks or cause process failures through SRB, hence organizations want to reduce these loss events and try to improve the security awareness of their employees.

2.2. ISA Delivery Methods

Security awareness is defined as" a state where users in an organization are aware, ideally committed to, of their security mission" (Siponen 2000). The employees should understand the importance of information security and they should know their responsibilities. Finally the employees should act compliant to the ISP (Puhakainen and Siponen 2010). The relevance of ISA campaigns and trainings for reducing security threats has been proved so far (Eminağaoğlu et al. 2009). In particular, ISA programs consist of a bundle of methods to build employees ISA. According to (Abawajy 2012a), we categorize ISA delivery methods in conventional, instructor-led and online delivery methods. Table 1 indicates ISA delivery methods and their advantages and disadvantages (Abawajy 2012a).

Table 1 Advantages and Disadvantages of ISA Delivery Methods according to (Abawajy, 2012)

Categories	Delivery Methods	Advantages	Disadvantages
Conventional delivery methods	Posters, Stickers, Leaflets	+ periodic information security reinforcement	- message may be overlooked
	Employee Newspaper	+ can convey a number of messages at the same time + tracking methods	- message may be overlooked - often seen as spam
Instructor-led delivery methods	Formal presentations and Training	+ instructor is able to perceive nonverbal student cues + modify instructional methods accordingly + provide timely answers to student questions	- expensive - many users find it to be boring and ineffective - depends on the instructor
Online delivery methods	Intranet Articles	+ effective when users actually read them + cost effective	- undermined due to volume of emails and spam - reading email message does not mean the message has been understood and internalized
	Web-based computer security awareness training (WBT)	+ user-friendly and flexible models that enable users to enhance security awareness at their own pace + train users to an enterprise-wide standard	-users attempt to complete the sessions with minimal time or thought; - becomes monotonous - fails to challenge the user and - provides no dialogue for further elaboration - lack of self-motivation or feelings of isolation
	Security alert messages (e.g. screen savers, pre-logon messages, email messages)	+ everyone is guaranteed to see them at least once, which make them an ideal channel for conveying essential security awareness messages in a minute or less	
	mobile learning platforms (e.g. Social media)	+ monitoring of progress	- expensive - complex implementation
	Game-based delivery methods	+ it can challenge, motivate and engage the participants	- often does not specifically reflect the policy of the organization or organization's related security issues

Awareness building interventions have to be frequent and can be carried out in campaigns (Siponen 2000). Topics of interest are changing fast, because working environments (e.g. mobile devices) and threats (e.g. social engineering) are altering shortly (Kruger and Kearney 2006). Hence a continuous ISA building process is essential to increase employees' level of awareness (Puhakainen and Siponen 2010). So far little attention has been paid to the role of horizontal communication (informal communication) in the awareness building process. Hence the underlying research explores the role of communication, topics and delivery methods concerning ISA. ISA delivery methods are used to build a IT risk culture in the organization (Jahner and Krcmar 2005). In large organizations different subcultures exists (Kolkowska 2011a). These subcultures could be people from different professions, departments, other locations of the organization. There are three specific subcultures for a security compliance program: top management, information systems management and end-users. We focus on end users, because information security awareness programs focus on end users awareness and behaviors.

2.3. ISA Measurement and Control

Internal controls and evaluation mechanisms are necessary to control the operations of organizations (Ouchi 1979). There are technical, formal and informal interventions for information security and the controls of these interventions should complement each other to effectively control information security (Dhillon 1999). ISA programs are classified as informal interventions and previous research presented a measurement model based on the dimensions attitude, knowledge and behavior measured through a questionnaire on a scoring model (Kruger and Kearney 2006). Further the authors recommended few design requirements for measuring ISA, namely a comprehensive and complete question database, include data from the system (e.g. log files or data from incidents) and the measuring tool should be automated (Kruger and Kearney 2006). Further we explore how banking companies measure success of their ISA programs and how to control the real behavior of employees, because only such a measurement could reflect real improvement of the employee behavior.

2.4. Research Problem and Objectives

The above discussion has shown that failure to account for individual employee behavior has been repeatedly identified as a major problem for improving information security in banking organizations. Adding to this problem is our limited understanding about ISA programs including the effective use of diverse delivery methods to improve ISA among employees. Finally, it has been found that despite the significance of ISA building, far too many delivery methods are not controlled to understand effects and implications of remediation measures. Little empirical work has been conducted to establish the important associations between these dimensions. We now give two research objectives to guide the remainder of the paper.

First, we seek to provide a current account of the current diffusion level of ISA methods for a large scale international banking company covering a variety of sub-organizations.

Second, we seek to identify differences in terms of measuring and controlling employee ISA across the various sub-organizations.

3. RESEARCH METHODOLOGY

3.1. Research Approach

The research study is based on a sequential two staged mixed methods design (Venkatesh et al. 2013) with the preliminary results from the first qualitative stage presented in this paper. The explorative phase using a qualitative approach contributes to develop the research constructs and hypotheses. A qualitative approach is recommended in the early cycles of phenomena investigation (e.g. (Edmondson and McManus 2007)). In specific, interviews are considered as a useful form of data-gathering to identify contextual conditions as well as for theory-generation and refinement.

Based on the results of the qualitative study, a survey will be conducted to test the proposed research hypotheses, in the second stage. The qualitative research was carried out as a thematic analysis (Braun and Clarke 2006). The qualitative research studies the social world as it is and the world is viewed as an emergent process, which is created by individuals (Dhillon and Backhouse 2001). Hence, the epistemology of the research is interpretive paradigm.

3.2. Research context

The underlying research focuses on universal banks. Universal banks underlie several regulations in consideration of IT (Luthy and Forcht 2006). One of the most important regulations related to risk is the directive from the Basel Committee of Banking Supervision. After the enactment of Basel II, banks have to manage operational risk proactive and they have to build minimum capital reserves for these risks. To fit this target group, we selected a major international bank, which provided us with an access to its headquarters and all subsidiaries located in different countries in Europe. The research sites are autonomous sub organizations of this international banking group. These sites are independent in the sense of managing their information technology and designing their ISA programs. Therefore, these research sites ideally allowed us to explore and compare different security awareness building practices and views together reasons for design decisions such as cultural factors and their implications.

3.3. Data collection and analysis

We conducted first ten semi-structured qualitative interviews, which took place from July to September 2013 (see Table 2). The sampling of interviewees followed a systematic approach with the intent to interview the responsible information security or operational risk managers of each research site. The semi-structured interviews were conducted with the managers in German and English following an interview guide. On average they lasted for 35 minutes, were tape recorded and fully transcribed. In some cases we were able to complement the data with information obtained from documents (e.g. leaflets, posters, reports).

Table 2 Conducted semi-structured interviews by banking sites and roles

Roles / Site	Headquarter	Site A	Site B	Site C	Site D
Chief Information Security Officer	2 (FF)	1 (FF)	1 (TI)	1 (TI)	1 (TI)
Head of Operational Risk	2 (FF)	1 (FF)	1 (TI)	0	0

FF... Face-to-Face Interview; TI... Telephone Interview

Data were coded using content analysis to generate conceptual categories (Mayring 2003). In the first round, the research team inductively coded the interview data separately in order to generate specific conceptual categories. Based upon Mayring's method, the coders' first defined relevant text passages in their materials as units of analysis, paraphrased them, and then generalized them at a higher level of abstraction. Originally stemming from grounded theory, the basic goal of this procedure was to construct a reasonably sophisticated picture in each organisational unit.

4. PRELIMINARY RESULTS

4.1. Suitability of Research Sites

Our results confirmed that all researched sites develop and manage their own ISA programs. The banks started their ISA programs between 2007 and 2011. All respondents agree about the importance of an effective ISA program to mitigate IT operational loss events. One respondent mentioned that "money is data in our systems", therefore confidentiality, availability and integrity of data and data assets are especially vital. In the organizations, the Chief Information Security Officers (CISO) develop, implement and monitor the ISA program in cooperation with the Marketing and PR departments.

4.2. End User Behavior

"They know about and they are able to speak about information security. If you ask me if their behavior is in accordance with ISP, then my answer is no or not always." (CISO)

The respondents mentioned that employees know what they have to do, but their actual behavior often not reflects this knowledge. The respondents are convinced that the ISA programs are good as they are now, but they have no adequate tools to measure ISA. Hence we assume that the level of awareness could not be known by the respondents. The respondents do not differentiate in designing ISA programs for different security behavior types. In some cases we screened the ISA materials and the most content concentrated on SCB and SRB of employees, because the leaflets and articles were provide the basic points of ISP.

4.3. ISA Delivery Methods

Mostly the entire CISOs plan the ISA program in form of a campaign combined with single interventions (E-Learning, intranet articles) distributed over the year. An ISA campaign takes almost one month and focus on few actual key aspects. ISA programs need additional resources to the budget of IT, hence top management approve budgets for the programs.

The researched banks use compared to numerous possibilities only few different ISA delivery methods, therefore they have a low diffusion level of ISA delivery methods. The basis for every ISA program is the intranet. The intranet offers articles of actual and past information security topics. In the intranet the ISP and desirable operating instructions are downloadable and employees have to know the ISP at their organizational entry. At their entry, the employees have to do an E-Learning course and pass an exam afterwards. Moreover, in three of five banks the employees yearly have to successfully complete an E-Learning course and exam. Table 3 provides an overview about the used delivery methods in the researched banks.

Table 3 Collection of ISA delivery methods of banking sites

Categories	Delivery Methods	Headquarter	Site A	Site B	Site C	Site D
Conventional delivery methods	Posters, Stickers, Leaflets		Y & SM	Y & SM		-
	Employee Newspaper	Y & NM		Y & NM	Y & NM	-
Instructor-led delivery methods	Formal presentations and Training	O & SM	-	-	Y & NM	-
Online delivery methods	Intranet Articles	B & SM	-	Q & NM	M & NM	Q & NM
	Web-based computer security awareness training (WBT)	Y & SM	Y & SM	Y & SM	O & SM	O & SM
	Security alert messages (e.g. screen savers, pre-logon messages, email messages)	-	-	-	-	-
	mobile learning platforms (e.g. Social media)	-	-	-	-	-
	Game-based delivery methods			Y & SM		

Y… Yearly, Q.. Quarterly, M… Monthly, B… Biweekly, W… Weekly, O… Once at organizational entry
SM... Success Measured, NM… Not Measured

The ISA programs consist of most important information security topics like secure password, secure internet usage, e-mail attachments and clean desk policy. Actual topics for this year's campaigns are social engineering, mobile devices and phishing. One respondent analyzed the page views of intranet articles and the most clicks got an article about Facebook as a hazard. The CISO's have no strategy to actively enforce informal communication about information security. We assume that a focus on the enforcement of horizontal communication could have positive effects on existing ISA programs. Some of the researched banks have implemented latest software to protect themselves from loss events (e.g. data leak prevention software, password evaluation software).

4.4. ISA Measurement and Control

The banks ISA measurements are simple and not automated. No bank uses a scoring model as it was stated by (Kruger and Kearney 2006). The researched organizations mainly analyze data from their log files out of their information system. The respondents agreed that the potential for automatic controls in the area of ISA is not exhausted right now, especially automatic controls in the business processes. One respondent developed a minimum operational security standard, which maps the risks of the processes.
All researched organizations conduct a survey after the employees finish the E-Learning course. The banks require every employee to do the survey, because for them the online test is the best possibility to measure knowledge of the employees. In addition, the number of page views published intranet articles is measured only by one CISO. Normally 4.000 to 6.000 of all together 11.000 employees read the intranet articles. There is no monitoring if the employees really got the meaning of the article. By contrast, one of the researched banks has conducted a social engineering penetration test last year to measure the effectiveness of their ISA program on phishing. They sent a phishing mail, which looks really similar to the mail of IT support of the bank, to the employees and asks them to send their passwords back. Only few employees react on this phishing mail and sent their passwords. Additional they left USB flash drive in the building (e.g. cafeteria, elevator) and also few employees try to use the flash drive after they found them. We define this measurement as proactive ISA controlling approach, because through the active involvement of employees ISA is created by the controlling method itself. Secondly, a key risk indicator for SRB is set up through a proactive ISA controlling approach. We assume that these experimental proactive forms of ISA measurement and controlling could have great potential to identify undesirable behavior of employees.

5. CONCLUSION

Our research has found out that the diffusion level of ISA programs and delivery methods in the researched banks is low. Most ISA programs use basic online delivery methods, like intranet articles, leaflets and posters, to build ISA of their employees. The most effective currently used method to build awareness and to measure the success is an E-Learning program with an exam afterwards. We assume that the low frequency of E-Learning interventions per year is not enough to effectively build awareness of the employees. Most of the banks investigated in the study mix some ISA delivery methods but the measurement of the effectiveness and the controls of the methods only exist on a very basic level and focus on knowledge repetition (e.g. quizzes). We propose to analyze proactive ISA controlling methods to increase desired behavior of

employees and therefore prevent IT operational loss events. A proactive ISA controlling method could be similar to social engineering penetration tests, in which the information security department simulates real attacks and evaluate the behavior of the employees in a real setting.

Further research uses the theory of planned behavior to analyze the influence of perceived ISA programs, perceived security culture and perceived security monitoring controls on employees' security behavior (SAB, SCB, SRB, SDB). The research should measure the research constructs' effects on employees' behavioral intention. An online survey will be conducted in every research unit. Intercultural differences in the field of ISA and security behavior will be investigated. Moreover, future research focuses on the impact of more sophisticated ISA controls on employees' security behavior and the effectiveness of viral ISA videos in order to change security behavior.

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2013. "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

References

Abawajy, J. 2012. "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*), pp 1-12.

Bauer, S., and Bernroider, E. Year. "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from exploratory Case Study," Proceedings of the International Conference Information Systems 2013, IADIS Press Lissabon, 2013, pp. 30-38.

Braun, V., and Clarke, V. 2006. "Using thematic analysis in psychology," *Qualitative Research in Psychology* (3:2), pp 77-101.

Chang, A. J.-T., and Yeh, Q.-J. 2006. "On security preparations against possible IS threats across industries," *Information Management & Computer Security* (14:4), pp 343-360.

Dhillon, G. 1999. "Managing and controlling computer misuse," *Information Management & Computer Security* (7:4), pp 171-175.

Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* (11:2), pp 127-153.

Edmondson, A., and McManus, S. 2007. "Methodological Fit in Management Field Research," *Academy of Management Review* (32:4), pp 1155-1179.

Eminağaoğlu, M., Uçar, E., and Eren, Ş. 2009. "The positive outcomes of information security awareness training in companies – A case study," *Information Security Technical Report* (14:4), pp 223-229.

Furnell, S., and Thomson, K.-L. 2009. "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security* (2009:2), pp 5-10.

Goldstein, J., Chernobai, A., and Benaroch, M. 2011. "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories," *Journal of the Association for Informaton Systems* (12:9), pp 606-631.

Guo, K. H. 2013. "Security-related behavior in using information systems in the workplace: A review and synthesis," *Computers & Security* (32), pp 242-251.

Jahner, S., and Krcmar, H. Year. "Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management," Americas Conference on Information Systems (11th AMCIS), Paper 462, Omaha, NE, 2005.

Kolkowska, E. Year. "Security Subcultures in an Organization - Exploring Value Conflicts," The 19th European Conference on Information systems Helsinki, 2011, p. Paper 237.

Kruger, H. A., and Kearney, W. D. 2006. "A prototype for assessing information security awareness," *Computers & Security* (25:4), pp 289-296.

Luthy, D., and Forcht, K. 2006. "Laws and regulations affecting information management and frameworks for assessing compliance," *Information Management & Computer Security* (14:2), pp 155-166.

Mayring, P. 2003. *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, (8. ed.) Beltz: Weinheim.

Ouchi, W. G. 1979. "A Conceptual Framework for the Design of Organizational Control Mechanisms," *Management Science* (25:9), pp 833-848.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp 757-778.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. 2009. "The impact of information richness on information security awareness training effectiveness," *Computers & Education* (52:1), pp 92-100.

Siponen, M. 2000. "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security* (8:1), pp 31-41.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of end user security behaviors," *Computers & Security* (24:2), pp 124-133.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conductiong Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp 21-54.

From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization

Abstract

Despite the importance of information security, far too many organizations, in particular banks, are facing behavioral information security incidents. In the context given by the headquarters of a large European banking organization, this single case study investigates whether individual behavioral compliance with the information security policy is influenced by accumulated security information and information security awareness embedded within the theory of reasoned action in an extended norms approach. We collected empirical data through a three-staged process in which we conducted semi-structured interviews, implemented a survey to test the developed research hypotheses, and engaged in interactive presentations to discuss the results. In particular, the qualitative interviews strengthened internal validity of survey constructs related to neutralization techniques and internal channel use for information acquisition. We found that the attitude toward information security policy compliance, and not only social norms but also personal norms related to neutralization techniques, are all significant variables potentially mitigating the knowing-doing gap reported in related information security research. Besides emphasizing the importance of extended norms, which should be accounted for in information security awareness programs, we also highlight the use of internal and external channels to acquire information as initial drivers of awareness. The empirical findings provide implications to practice and advance theoretical development by generally supporting the developed model that accounts for compliant information security behavior at an international bank.

Keywords: Information Security Awareness, Information Security Policy, Compliant Information Security Behavior, Theory of Reasoned Action, Neutralization Theory, Banking.

Introduction

The current modern business climate suffers from a diverse range of threats to corporate data, technical infrastructures, operating systems, and applications (Johnston and Warkentin 2010). Banking organizations in particular are not only dependent on these information technologies (IT) but also confronted with an increased frequency of IT-related security incidents with critical consequences, including financial and non-financial losses (PricewaterhouseCoopers 2014). A substantial proportion of these security incidents comes from inside the bank and can be attributed to individual, undesirable behaviors with the potential to jeopardize critical information systems and assets belonging to the organization (Abu-Musa 2006). Consequently, in an effort to mitigate related risks, banks introduced operational risk management, which is now a regulatory requirement since Basel II (Ciborra 2006; Hsu et al. 2013a). In this context, information security is regarded as a critical means of ensuring the availability, confidentiality, and integrity of information and related assets of an organization, and therefore it helps to prevent operational loss events (Goldstein et al. 2011).

The individual user is the predominant weakness when it comes to developing information security in organizations (Ifinedo 2012; Pfleeger and Caputo 2012). Information security (IS) research has only begun to recognize the importance of employee behavior in this context (Crossler et al. 2013; Hsu et al. 2013a; Im and Baskerville 2005; Liu and Vasarhelyi 2014), particularly with regard to compliance (Bulgurcu et al. 2010; Pahnila et al. 2007; Siponen et al. 2010; Warkentin et al. 2011). One essential tool for shaping user behavior is to define and communicate an information security policy (ISP) where mandatory organizational rules, guidelines, and requirements are laid out. The ISP determines compliant information security behavior with regard to confidential information handling and the expected norms of information systems usage (Warkentin and Willison 2009). The ISP is a key control for supporting information security in banks (Bulgurcu et al. 2010), and even its existence appears to have a positive effect on employee perceptions of their need to comply (Boss et al. 2009). Allowing employees to understand the ISP is believed to be one of the most cost-effective means of reducing information security risks (Dhillon 1999; Hagen et al. 2008; Parsons et al. 2014; Siponen 2000). It has been suggested to use individual knowledge related to the ISP as a potential metric to measure various stages of ISP compliance in organizations (Pahnila et al. 2013).

Consistent with these views, banks are implementing programs to increase information security awareness (ISA) and related knowledge held by employees, thereby allowing them to understand information security and the ISP (Bauer et al. 2013a; Kajzer et al. 2014). Current areas usually covered by these programs include, for example, phishing, social engineering, password security, secure Internet use, and clear screen policies (Quagliata 2011). However, loss events resulting from non-compliant information security behaviors due to deliberate or non-deliberate acts (Willison and Warkentin 2013) are still common (Boss et al. 2009; Warkentin and Willison 2009). Non-deliberate acts such as careless behavior can be further exploited by external perpetrators or internal violators, who can use these breaches to conduct attacks and gain access to confidential information (e.g. copy customer data) (Connelly et al. 2011). Other typical examples of non-compliance are the installation of malware, uploading confidential data to a mobile device, or visiting unsecure websites (Siponen and Vance 2010). These actions are non-deliberate if employees are unaware of the ISP of their organization or do not understand its rules and procedures (Cox 2012). Cognitive justifications accompanying behavior are common in the case of deliberate non-compliance in organizations (Minor 1981; Sykes and Matza 1957). The basic idea is that people personally free themselves from the moral constraints of ISP requirements so that they may then choose to act in non-compliant ways. In finding excuses, employees may temporarily neutralize certain values before violating ISPs, by, for example, denying any responsibility for the situation (Siponen and Vance 2010).

Despite recent calls for more empirical evidence building on behavioral theories to explore the persistent phenomena of employee non-compliance with ISP (Crossler et al. 2013), little empirical research has systematically addressed how ISA is fostered by individually accumulating related information and whether ISA impacts reasoned ISP compliant action mediated by attitudes and norms, in particular in highly sensitive financial institutions. To target these research questions, we developed a new research model drawing from behavioral theories that have been separately applied in the extant information security literature, albeit to different degrees. Considering the relevance of knowledge in forming behavior (Baranowski et al. 2003; Khan et al. 2011), the research model applied to an international bank first highlights the role of employees' use of internal and external channels to acquire information and thereby develop ISA. Extending beyond previous studies that focus on how ISA impacts specific security behavior (Eminağaoğlu et al. 2009), this

study then acknowledges the mediating roles of the users' perception of extended norms besides considering personal attitudes. With extended norms, we refer to both social and personal norms, which have been insufficiently considered in the existing security literature (Sommestad and Hallberg 2013) drawing on the Theory of Reasoned Action or Theory of Planned Behavior (TRA/TPB) (Ajzen 1985; Ajzen 1991b; Fishbein and Ajzen 2010). While we also have adopted this well-supported predictive persuasion perspective, we extend previous work limited to specific norms, either personal (Li et al. 2010) or social (Herath and Rao 2009a; Herath and Rao 2009b), by implementing an "additional norms approach" (White et al. 2009). Subjective norms are extended to social norms, and personal norms are represented by neutralization techniques (Sykes and Matza 1957), which were only recently acknowledged to study information security behavior (Barlow et al. 2013; Siponen and Vance 2010).

In terms of methodology, we conducted a positivistic case study based on a single case for theory testing purposes, which combined different data collection techniques (Eisenhardt 1989; Yin 2014). In our main research stage, we implemented a survey at the headquarters of a large international bank and performed a partial least squares structural equation modeling (PLS-SEM) analysis to validate measurement and test nine hypotheses (Wold 1982). Our findings should, therefore, offer rare insights into a sensitive area with high internal validity at a normally well-sealed financial institution.

Theory development and research motivation

This section briefly introduces the main terms and theories and summarizes results of previous research needed for understanding and developing the research model and hypotheses.

Information security awareness (ISA)

Several scholars have argued that employees' information security awareness (ISA) is one of the most important ingredients for achieving the goals of information security in organizations (D'Arcy et al. 2009; Siponen 2000; Thomson and von Solms 1998). ISA can be defined as "a state where users in an organization are aware of – and ideally committed to – their security mission" (Siponen 2000, p. 31). This definition recognizes a cognitive state in which the individual perception about information security within the organizational context is relevant and is traditionally framed by information security policies (ISP). Therefore, other broader definitions of ISA explicitly mention both knowledge or recognition of information security, and the organization's ISP (Bulgurcu et al. 2010; Rocha Flores and Antonsen 2013; Siponen 2000). Both aspects are essential for being risk aware. Not surprisingly, Pahnila (2013b) confirms that an employee's ISP knowledge affects how intentions to comply with the ISP are formed. Moreover, ISA is temporal, and it must be renewed frequently with ISA programs (Wilson and Hash 2003). Especially organizations from the financial sector have followed this advice by regularly "refreshing" related ISA in the context of strict ISPs (e.g. through e-learning initiatives and mandatory quizzes) (Bauer et al. 2013a). Consequently, we conceptualize ISA as employees' cognitive ability to recognize and understand information security threats and risks in the context of their organization's ISP.

Due to the recognized importance of ISA, recent research in the IS field has begun investigating ways to improve ISA (Albrechtsen and Hovden 2010; Eminağaoğlu et al. 2009; Hagen et al. 2008; Kajzer et al. 2014; Khan et al. 2011; Tsohou et al. 2015). In practice, different methods are usually bundled into coordinated campaigns termed ISA programs (Kajzer et al. 2014; Quagliata 2011; Tsohou et al. 2015) to deliver relevant security information and knowledge to all organizational users of information systems (Wilson and Hash 2003). The applied internal channels for information acquisition can include conventional approaches, instructor-led approaches, and online approaches (Abawajy 2012b). As observed in a recent global case study about a large international bank with multiple locations (Bauer et al. 2013a), conventional approaches included internal newspapers, leaflets, posters, and printed coffee cups. Instructor-led approaches were implemented as mandatory employee induction workshops covering compliant information security behavior according to the bank's ISP. Online approaches were implemented and shared via the intranet, which was used as a preferred communication channel for alerts and e-learning activities, and also as an online repository for accessing the ISP.

Prior research classifies the nature of ISA programs as informal controls meant to alert employees to potential information security risks, often by communicating the content of formal controls (Albrechtsen and Hovden 2010; Kajzer et al. 2014). While formal controls such as the ISP or working instructions are specified material entities, informal controls aim to establish an appropriate security culture and the social injunctive norms needed to improve compliant information security behavior (Van Niekerk and Von Solms 2010). Formal and informal controls act in tandem to improve information security (Dhillon 1999). Used on their own, technical controls such as intrusion-detection systems or access controls are not sufficient to assure the confidentiality, availability, and reliability of information and data in organizations (Warkentin and Willison 2009). Simple behaviors such as writing down passwords or uploading confidential information using an unsecure connection can make technical controls ineffective (Siponen 2000; Thomson and von Solms 1998).

Behavioral theories

Current academic literature recommends using behavioral theories to investigate information security for a number of reasons (Khan et al. 2011; Lebek et al. 2014). Among other advantages, they permit deeper consideration of the resources and motivators behind the behavior at issue, shed light on how these factors interact in an integrative model, and illuminate which interventions can be used most effectively to influence the behavior in question (Donovan 2011).

The theory of reasoned action (TRA) offers a well-supported predictive persuasion perspective on individual behavior (Fishbein and Ajzen 1975; Fishbein and Ajzen 2010). According to the TRA, individual intentions to perform a behavior are a function of two basic variables, one personal in nature (attitude toward the

behavior) and the other determined by social influence (subjective norms), which reflects the amount of pressure that individuals perceive they are under from significant others to engage or not to engage in the behavior. This model is applicable to any situation in which individuals consciously form intentions that directly lead to behavior under volitional control of the individual. In situations where the behavior being studied is not completely under the control of the individual, the Theory of Planned Behavior (TPB) (Ajzen 1985; Ajzen 1991b) is applicable, which in addition includes a self-efficacy related measure of perceived behavioral control that has both an indirect effect through behavioral intentions and a direct effect on behavior. Evidence was provided showing that attitudes (Bulgurcu et al. 2010; Hu et al. 2012; Siponen et al. 2014c), subjective norms (Cox 2012), and perceived behavioral control (Hu et al. 2012; Ifinedo 2012) can all be valid predictors of information security behavior. The relative importance of these predictors, however, is expected to vary across behaviors and situations (Ajzen 1991b). Moreover, the direct intention-to-behavior link also was confirmed for the information security compliance context (Lebek et al. 2014; Sommestad and Hallberg 2013).

Since the original publication of Wicker's (1969) conclusion that attitudes alone do not predict intentions, additional integrated models of behavior were developed over the last decades to improve the predictive power of these models. While a social influence conceptualization in terms of subjective norms was consequently included in the popular TRA/TPB to complement personal attitudes, contemporary research suggests that further norms may be warranted to increase the variance explained by its constituent predictors (Rivis and Sheeran 2003; White et al. 2009). The subjective norm component of the TRA/TPB is a social injunctive norm, as it is concerned with social pressures from others to perform the behavior in question and therefore highlights the social rewards and punishments for performing or not performing the behavior (White et al. 2009). It can, however, be extended to also include a descriptive norm and include what is typical or normal in the social context, which was suggested in the Integrative Model of Behavioral Prediction (Fishbein 2000). This model suggests a differentiated reflection of norms, including perceptions of what others think one should do (social injunctive norm) as well as perceptions of what others are doing (descriptive norm). In addition, further research has argued to include personal injunctive norms reflecting one's internalized moral rules (Parker et al. 1995) in predicting behavioral intentions (White et al. 2009). Personal injunctive norms measure one's self-approval (or disapproval) of the behavior in question and have been found to be of particular importance to predict behaviors with a moral component.

In criminology theory, Neutralization Theory emerged in the 1960s as a well-established theory providing a means of analyzing the deviant behavior of adolescents (Minor 1981; Sykes and Matza 1957). In essence, this theory draws on a special kind of personal injunctive norms related to neutralization techniques that people use to justify and excuse their deviant behavior for themselves and possibly others (Sykes and Matza 1957). Recent decades have seen heavy use of Neutralization Theory in health research (Maruna and Copes 2005). Thus far, only a few studies have linked information security compliance with Neutralization Theory, and call for more work to confirm the effects of neutralization techniques on compliant employee information security behavior (Barlow et al. 2013; Siponen and Vance 2010). In principle, employees may use neutralization techniques to justify ISP violations. Typical neutralization techniques can be related to time and work pressures, perceived unjust rules, and a poor understanding of risks and possible threats (Siponen and Vance 2010). The original theory was based on five techniques of neutralization (Sykes and Matza 1957), but over the decades four additional techniques of neutralization have been identified (Lanier et al. 2004). 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).

The link between knowing and doing

Extensively researched by social psychologists are constructs of attitude-relevant knowledge, which can be explained as the attitude-relevant beliefs and experiences that come to one's mind when encountering an attitude object (Davidson et al. 1985; Fabrigar et al. 2006). These beliefs and experiences about the attitude object have important implications for attitudes and behavior (Fishbein and Ajzen 1975). The process of change in behavior triggered by changes in attitude-relevant knowledge was summarized in the Knowledge, Attitude and Behavior (KAB) model (Baranowski et al. 2003; Chaffee and Roser 1986; Khan et al. 2011; Parsons et al. 2014). This model draws from extensive research on attitudinal properties, more specifically attitude-relevant knowledge and the important role of knowledge in determining evaluative judgments (Allport 1935; Campbell 1963). Studies from sectors such as healthcare (Baranowski et al. 2003) have

convincingly demonstrated that according to the KAB model, changes in attitude are initiated as individual knowledge accumulates. This offers a useful theoretical lens implicating that attitude-relevant knowledge acts as a logical prerequisite for behavioral change. Recent work has highlighed the important role of individual knowledge for information security. For example, it was shown how knowledge influences persuasion through changed attitudes toward compliant information security behavior (Bulgurcu et al. 2010; Parsons et al. 2014) and that ISP knowledge influences how intentions for compliant information security behavior are formed (Pahnila et al. 2013b). However, there seems to be a consistent knowing–doing gap in behavioral information security research (Cox 2012), which reinforces the need for models, in particular in terms of our approach, offering more than just attitudes mediating the effects of knowledge.

Research model development

In the proposed research model shown in Figure 1, we propose that the individual acquisition of information on information security through internal and external channels translates into improved ISA and that an improved ISA is related to improved attitudes and norms positively impacting information security behavior via intentions. Our research conceptualization is new, yet consistent with the introduced TRA, Neutralization Theory, and the KAB model. The following subsection elaborates on the choice and integration of models. We then develop the postulated relationships in terms of research hypotheses.

Choice and integration of models

We chose to test the widely accepted TRA (Fishbein and Ajzen 1975; Fishbein and Ajzen 2010) and not its extensions, the TPB (Ajzen 1985; Ajzen 1991b), in combination with an additional norms approach. The TRA was deemed to fit our context, as the targeted users in the case study are able to self-regulate their information security behavior. Prior information security studies have confirmed that when the behavior in question is more volitional in nature, the effects of perceived behavioral control (PBC), the added antecedent of behavior in the TPB, are weaker (Sommestad and Hallberg 2013). Our initial interviews suggested that the desired security behaviors are under an individual's control and not technically complex. Hence, the original TRA fits well to our practical situation where there are no realistic constraints affecting the behavior (Armitage and Conner 2001; Roberts and Henderson 2000). Therefore, we decided to focus on attitudes and extended norms in our research model, and consider PBC as a control variable only.

Consistent with the "additional norms approach" in TPB/TRA research (White et al. 2009), we first propose integrating neutralization techniques as a special case of personal injunctive norms in the research model. Neutralization techniques reflect personal moral justifications to oneself to engage or not engage in behavior, here specifically related to non-compliant information security behavior (Li et al. 2010; Siponen and Vance 2010). Neutralization techniques should, therefore, extend the variance explained in behavioral intentions. It allows for including personal moral norms known to explain volitional non-compliant information security behaviors. Personal norms in terms of more general personal moral standards were identified to strongly affect individual compliance intention related to Internet use policies (Li et al. 2010). With neutralization techniques, we can test whether employees neutralize their internalized personal norms, leaving them free to possibly engage in non-compliant or delinquent acts. Second, we follow Fishbein's recommendation (2000) to extend the subjective norm in TRA into social norms to include both social injunctive and descriptive norms. In other words, users should account for both the social pressure induced by others and the perception whether other people conduct the behavior in question, respectively (White et al. 2009).

Finally, we adapt the idea behind the knowledge, attitude, and behavior (KAB) model, which assumes that knowledge is the precondition for any conscious self-regulatory process (Chaffee and Roser 1986). We propose that employees' accumulated knowledge should enhance employees' ISA, which should impact attitudes toward ISP compliance (Bulgurcu et al. 2010). Therefore, we analyze the role of internal and external channels to acquire information and thereby contribute to understanding how attitude-relevant knowledge is established (Baranowski et al. 2003; Khan et al. 2011; Parsons et al. 2014).

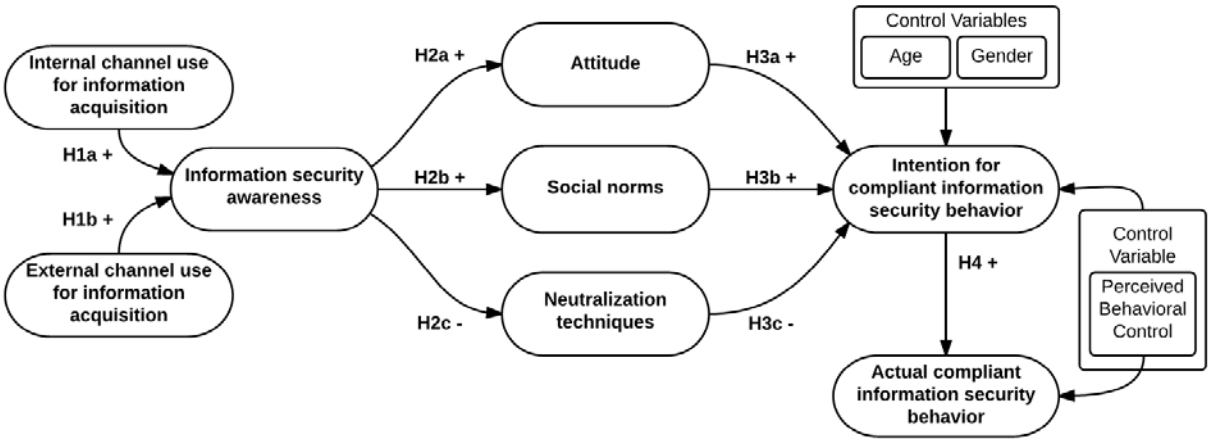


Figure 5. Research model

The role of channel use for information acquisition

In our research model, we first consider the role of employees' use of internal and external channels for information acquisition, which should positively impact ISA of employees. Employees can acquire security information internally through channels provided by their organization (Bauer et al. 2013a), or by using a range of different external channels (Craig and Allen 2013). Previous research suggests that it is information processing through which individuals acquire relevant information related to evaluating and conducting behavior (Campbell 1963; Fishbein and Ajzen 1975). However, the specific sources for the manipulation of ISA and implications in the information security context are not sufficiently understood. A recent study suggests that text-based, game-based, and video-based methods are effective in building ISA seen as learnt states through which individuals derive consistent, compliant information security behaviors (Abawajy 2012b). These and other methods can be part of organizational ISA programs, which should be carefully designed to understand their overall levels of effectiveness in fulfilling their purpose (Albrechtsen and Hovden 2010; Hagen et al. 2011). One important aspect is the provision of information about the ISP and related instructions (Thomson and von Solms 1998), in particular on an iterative basis. Literature suggests to regularly send reminders to users about current information security risks and threats, such as phishing attacks or careless behaviors concerning passwords (Wilson and Hash 2003). This iterative process targets the individuals' level of attitude-relevant knowledge of threats and risks in the context of the ISP. Consequently, we propose that the individual utilization of different channels in the area of information security should be valuable for developing ISA. As related studies have not differentiated between internal and external channel use (Abawajy 2012b), we propose two separate hypotheses:

H1a-b: ISA is positively affected by internal (a) and external (b) channel use for information acquisition.

The role of information security awareness (ISA)

Next, we highlight the central role of ISA for reasoned compliant action in relation to the ISP. Consistent with the important role of information processing (Fishbein and Ajzen 1975) and our working definition of ISA reflecting a cognitive state, we reason that, as ISA increases, related employees' cognitive processes and beliefs about information security will change as a consequence (Bulgurcu et al. 2010). Through ISA, employees should become more cognizant of risks related to information security, which should eventually translate into changed attitudes and norms. In an information security context, only a few studies have considered these relationships in an integrated analysis (Sommestad and Hallberg 2013). As ISA reflects IS related knowledge, it should be a precondition for any conscious self-regulated IS behavior (Chaffee and Roser 1986), which in our predictive persuasion perspective given by the TRA (Fishbein and Ajzen 1975; Fishbein and Ajzen 2010) is preluded by affected attitudes. Recent IS studies have indeed shown that IS related knowledge has a strong effect on attitudes (Parsons et al. 2014), and that specifically ISA has a direct influence on forming favorable or unfavorable attitudes toward information security compliance (Bulgurcu et al. 2010). These attitudes can then be seen as behavioral dispositions resulting from learning and information processing (Campbell 1963). Consequently, we assume:

H2a: ISA has a positive effect on attitudes.

In addition to attitudes, we also postulate that ISA affects social and personal norms as predecessors for behavioral intentions. The pilot study of Merhi and Midha (2012) indicated that threat appraisal training has significant positive effects on descriptive norms, which is a dimension of social norms. Other findings highlight the importance of collective reflection and discussions concerning information security (Albrechtsen and Hovden 2010; Bauer et al. 2013a), which should eventually lead to improved social norms. Hence we assume:

H2b: ISA has a positive effect on social norms.

It was reported that delivering IT-security information to work against neutralization techniques or highlight deterrent sanctions is effective at reducing neutralization techniques and changing personal norms (Barlow et al. 2013). In this sense we seek to highlight the mediating role of ISA positioned in-between and governing the relationship between channel use for information acquisition and changed personal norms, which in this study we relate to the use of neutralization techniques. As ISA increases, employees should be less likely to morally excuse non-compliant information security behavior via neutralization techniques (Siponen and Vance 2010). Hence, we propose:

H2c: ISA has a negative effect on the use of neutralization techniques (and therefore has a positive effect on personal norms).

The role of attitudes and norms

We propose that the antecedents of our research model introduced through a combination of TRA and extended norms influence behavioral intentions. This first includes the attitude, which according to early theorists, is a behavioral disposition to respond in a particular way. An attitude was defined as "a mental and neural state of readiness ... exerting a directive or dynamic influence upon the individual's response to all objects and situations with which it is related" (Allport 1935, p. 810). Related prior studies have generally confirmed the relevance of attitudes as an inclination for a directional response toward compliant information security behavior (Bulgurcu et al. 2010; Cox 2012; Guo et al. 2011; Pahnila et al. 2007b). Hence, we assume:

H3a: Attitudes have a positive effect on the intention for compliant information security behavior.

Social norms are the result of normative beliefs (Fishbein and Ajzen 2010) and should positively impact ISP compliance intentions (Herath and Rao 2009a; Merhi and Midha 2012). Social norms are defined as employees' perception of an acceptable or permissible ISP compliant behavior within their organization (Fishbein and Ajzen 2010). These norms are a result of the organization's security culture, which was associated with improved employee information security behaviors (Hu et al. 2012). Related work has shown that workgroup norms in general impact the intention for non-malicious security violations in the workplace (Guo et al. 2011). A recent literature review from Sommestad and Hallberg (2013 generally confirmed the positive effects of social norms on behavioral intentions but also noted that these effects are marginally lower when the behavior in question is tied to ISP compliance in comparison with violation. Hence, we propose:

H3b: Social norms have a positive effect on intention for compliant information security behavior.

Now we turn to personal norms conceptualized as neutralization techniques. Neutralization techniques are defined as justifications, which individuals invoke to convince themselves, and others, that their deviant behaviors are justifiable and/or excusable (Siponen and Vance 2010; Sykes and Matza 1957). If employees engage in such justifications, then this should have a negative impact on their intentions for compliant information security behavior. This assumption was confirmed in a recent study related to the context of information security policy compliance (Siponen and Vance 2010), which has also shown that the effects of informal or formal sanctions are negligible compared to neutralization. The relationship was also confirmed in the context of cyberloafing, where employees use their Internet access at work illegitimately and secretly for private purposes (Lim 2002). Private Internet use in the workplace seems to be strongly affected by neutralization techniques and its perceived benefits (Cheng et al. 2014). Moreover, personal moral norms

was reported to explain more variance of the intention to comply with Internet use policies than perceived risks and perceived benefits to comply (Li et al. 2010). In an older study, the use of the neutralization technique "denial of responsibility" was positively correlated with intentions to commit computer abuse (Harrington 1996). We add to these studies by seeking to confirm the relationship in our context and contrast the influence of neutralization techniques as a personal norm with social norms. Hence, we propose:

H3c: Neutralization techniques have a negative effect on the intention for compliant information security behavior.

Finally, we seek to revisit the intention-behavior link in our study's context, which was already confirmed by previous studies (Lebek et al. 2014; Siponen et al. 2014c; Siponen et al. 2010; Sommestad and Hallberg 2013). We adapted the definition of the construct intention for a compliant security behavior (ICSB) from Siponen et al. (2014c, which claims that ICSB is an employee's intention to engage in compliant information security behavior. Similar to that, the level of an employee's perception of actual compliant information security behavior is represented by the construct actual compliant security behavior (Siponen et al. 2014c). Hence, the following hypothesis is proposed:

H4: Intention for compliant information security behavior has a positive effect on the actual compliant information security behavior.

Research methodology

This research can be classified as a positivistic case study based on a single case for theory testing purposes (Eisenhardt 1989; Yin 2014). By means of a survey, we quantitatively tested a causal research model developed from theory complemented by pre-survey data collection to explain how compliant IS behavior in the case organization unfolds. Thereby, we seek to confirm and potentially extend existing theory considering the conditions of a specific large banking organization. Post-survey meetings followed to validate its usefulness to members of the case organization (Pare 2004). The next subsections provide more details on the applied research methodology.

Case selection and information

In selecting the case, we followed a purposive sampling technique to identify a critical case to test theory within a real-life context of an international bank (Yin 2014). The selected single case (using SecureBank as pseudonym) was deemed ideal for investigating the research questions in the context of a highly sensitive and usually much safeguarded domain. SecureBank is the central institution of a large European banking group operating in approximately ten countries with assets of more than 12 billion euros. As a highly diversified and international financial services institution, SecureBank provides banking products and services to individual end consumers, businesses, government agencies, and other financial institutions. Information security is considered a high strategic priority and an external compliance requirement (Bauer and Bernroider 2013b). Therefore, the bank is dependent on ISP programs as preventive control to foster compliant information security behaviors among employees. It also had a prior history of developing, communicating, and enforcing ISPs with different levels of success. Thus, management was very interested to support the study and approved the fieldwork, which thereby allowed us to gain insight into how to effectively develop employee ISA and ultimately improve information security through compliance with the ISP.

Data collection stages

The case study was conducted between January and July 2014 over three main stages. In the first explorative stage, we performed four face-to-face semi-structured interviews with two information security managers, a public relations manager, and a general security manager of the bank and reviewed internal materials. The main purpose of the interviews was to understand the context, develop the research aims, and clarify the intended research process and expected results. Both interviewed security managers have been employed in the bank for decades and regularly conduct information security trainings and meetings across the entire organization. Thus, their understanding of the organization and research context was essential in developing this study. The decision was made to develop and implement a survey targeting employees to understand to

what extent existing theory on ISP compliance applies to the organization. The development of the survey included the selection of applicable theories, and the refinement and validation of constructs. In the second main research stage, the developed research model was tested through an online survey targeting all 600 employees of the SecureBank's headquarters as units of analysis. The link to the questionnaire was published on the bank's intranet homepage, and emails were sent to all employees with an invitation to participate. The survey (following pre-tests) was kept open for two weeks. To ensure contextual relevance (Siponen and Vance 2013), the introduction explained central terms such as the information security policy (ISP) and the types of typical behaviors that can be considered as ISP violations (e.g. not ensuring clear screens, unsecure passwords). Once quantitative data had been collected, it was cleaned by excluding two cases of obvious aberrant response behavior. Incentives included a raffle with the chance to win two dinner tickets, for which almost half of the respondents registered. Finally, the third research stage concluded our field work with two meetings, where the usefulness of the research findings was analyzed and discussed. Table 1 summarizes the empirical research process. To complement data collection, we collected and analyzed further empirical evidence on organizational efforts to promote ISA.

Table 1. Data collection stages

Stage	Approach	Target person(s)	Date	Duration
1	Face-to-face interviews	Chief Information Security Officer (CISO)	8 Jan 2014	55 min.
		Group Security Officer	16 Jan 2014	65 min.
		Chief Information Security Officer (CISO)	14 Mar 2014	60 min.
		Public Relations Officer	16 Apr 2014	44 min.
2	Survey	Pre-tests: Three groups	20-30 Apr 2014	10 days
		Survey reflection and approval by CISO	04-06 May 2014	2 days
		Main survey: Headquarter employees	11-25 May 2014	2 weeks
3	Interactive Presentations	Chief Information Security Officer (CISO)	4 Jul 2014	62 min.
		Group Security Officer	16 Jul 2014	68 min.

Tests for establishing validity and reliability

Various test procedures are recommended in literature to establish validity and reliability (Riege 2003; Stuart et al. 2002; Yin 2014). To ensure a high level of internal construct validity, we applied data source and between-method triangulations by using multiple sources of data for the same issues, for example by interviewing different managers about ISP compliance and using various data gathering methods (survey, interviews, and documents) at different research stages (Yin 2014) and by complementing quantitative with qualitative data (Modell 2005). We reviewed established constructs from literature and consulted security managers to establish appropriate operational measures for theoretical concepts tested by the survey. The survey instrument was pre-tested, non-response bias was analyzed, and the fit of the measurement and structural models with the gathered data was carefully tested in terms of validity and reliability, following current guidelines (Hair et al. 2014).

We conducted 22 pre-tests divided into three stages, where the consistency and understandability of the questionnaire were tested and improved on an iterative basis. The first stage of pre-testing was carried out with six affiliates of our university who had no specific knowledge about the study. After accounting for their feedback, we eliminated five items, changed the orientation of three scales, and reworded seven items. After completing pre-test one, we fielded pre-test two in the case organization, limiting it to ten employees. The responses provided detailed comments that led to the modification of nine items. Finally, six more research associates were asked to fill out the questionnaire and identify problems, resulting in the identification of only a few concerns and prompting minor refinements to two items and instructions at the beginning of the questionnaire.

We investigated survey nonresponse bias using the commonly applied wave analysis (Van der Stede et al. 2006), where early versus late respondents are compared on the assumption that late respondents are more likely to resemble non-respondents (Moore and Tarnai 2002). Therefore, we divided the sample into two groups based on the time the response was registered with regard to the online survey implementation. Respondents who answered the online survey in the first 48 hours were classified as early respondents (N=40), and all others were classified as late respondents (N=57). There are no differences in the groups in terms of gender ($\chi 2$ test, p=.364), age (Mann-Whitney-U-Test, p=.542), job tenure (Mann-Whitney-U-Test, p=.289), and organizational tenure (Mann-Whitney-U-Test, p=.735). Thus, we conclude that non-response bias is not an issue. Moreover, two weeks after concluding the online survey, employees were asked about their reasons for not responding. Most non-respondents stated that they overlooked the invitation to participate or lacked the time due to current workloads.

Given survey data based on same-respondent replies, common method bias or common method variance (CMV) is generally also taken into account to consider validity and reliability (Malhotra et al. 2006 ; Podsakoff and Organ 1986). The mono-method survey design and self-report instrument may cause a certain amount of covariance shared among all indicators. To prevent potential CMV, we used a sequence of questions that discouraged participants from detecting certain relationships between the dependent and independent variables. To detect CMV, we applied the Harman's single-factor test as a diagnostic technique. It involves entering all constructs into a principal components factor analysis to see if either a single or a general factor emerges that may account for the majority of covariance among measures (Podsakoff et al. 2003). Nine factors emerged. The first accounted for 35.93% of the variance. The other eight (with eigenvalues greater than one) contributed to the remaining 40.36% of the variance explained by the set, each accounting for 10.38% to 2.72%. This suggests that while some CMV is likely, the effect can be considered as not serious.

External validity is concerned with the extent to which the findings of a particular study can be generalized across populations, contexts, and time (Modell 2005). For our study, we defined the context, scope, and boundaries of our research case and compared our findings with extant literature, building on similar theory and contexts to allow for a reasonable level of analytical generalization (Riege 2003). Consequently, we aim at generalizing results to the applied broader theoretical framework and the domain of highly regulated banking institutions (Yin 2014).

Survey instrument development

The process of construct development began with a review of MIS instruments with well-established psychometric properties in empirical literature followed by a careful selection of constructs fitting the definitions in our research model. The appendix provides the survey instrument (Table A1) with supporting references.

In the context of the TRA, we used established constructs for measuring the individual attitude (ATT) toward information security (Hu et al. 2012), and the intention for compliant information security behavior (ICSB) and actual compliant information security behavior (CSB) (Siponen et al. 2014c; Siponen et al. 2010). In terms of norms, we needed to depart from the subjective norm construct to fit our research design and establish a combined more general social norm construct (Fishbein 2000; White et al. 2009). The selection of items to cover both types of norms was based on a recent information security study validating a range of items for assessing information security in organizations (Rocha Flores and Antonsen 2013). This study also served to identify items to assess ISA in terms of an individual perception on information security within the given organizational context. Consequently, all developed instruments are reflectively measured constructs from prior information security research, which we validated again in our study.

In measuring the neutralization techniques representing personal norms, we followed the recommendation that certain dimensions of Neutralization Theory are applicable to specific contexts of research (Barlow et al. 2013). Previous studies in information security compliance research tested six (Siponen and Vance 2010) and three (Barlow et al. 2013) techniques of neutralization. We drew on semi-structured interviews with security managers in our exploratory research stage one (see Table 1) to establish which neutralization techniques are most applicable to our highly sensitive context of banking companies with binding ISPs. According to the interviews, the following four out of six given neutralization techniques (Barlow et al. 2013; Siponen and Vance 2010) apply to their employees in conjunction with ISP violations: "Denial of

responsibility" means that an employee does not feel responsible for her actions and thinks that her behavior is beyond her control. "Defense of necessity" refers to claiming that an employee has too little time to carry out the work. Downplaying the harm employees' non-compliant behavior causes is called "denial of injury". Finally, "Condemnation of the condemners" refers to employees' feelings that the rules are unjust or make no sense (Sykes and Matza 1957). The same four techniques were also used in a previous information security compliance study (Siponen and Vance 2010). As each single neutralization technique reflects a specific reason to justify non-compliant behavior, they do not necessarily need to correlate with each other and are not interchangeable. Consequently, we conceptualized the neutralization techniques as a formative construct consisting of one item for each technique causing the construct. To capture how information is gained to foster ISA, we also draw on two formatively measured constructs to capture the use of internal and external information channels. Again, the information channels used to gain information were derived from the acquired context data via interviews and the assessment of internal artifacts. In terms of internal channels, we also consulted another study on the banking context (Bauer et al. 2013a), and in terms of external channels we complemented our analysis with a current media study (Craig and Allen 2013).

Survey sample characteristics

Table 2 shows sample characteristics of our survey. The sample consists of an almost equal number of male and female respondents. More than two-thirds of employees are between 30 and 50 years of age and have a job tenure between 11 and 30 years, with an organizational tenure between 0 and 20 years. Job tenure refers to the number of years of work experience.

The survey yielded 97 valid returns corresponding to a 16.2 % response rate, which is sufficient for data analysis according to current PLS-SEM recommendations (Hair et al. 2014). While the low minimum sample size requirement is among the most cited reasons for using PLS-SEM, it is still recommended to consider it against the given model and data characteristics (Hair et al. 2014; Lowry and Gaskin 2014). In our model, the maximum number of independent variables in any structural path is three. Therefore, assuming the commonly used level of statistical power of 80%, we need at least 59 data sets for detecting R2 values of at least 0.25 with an error probability of 5%. According to the often cited 10 times rule (Barclay et al. 1995), our recommended minimal sample size is 40, given by 10 times the maximum number of formative indicators used to measure a construct. Moreover, our sample offers unique and real insights into a traditionally highly protected and closed banking organization and, therefore, offers added value to many related studies building on student samples (Dinev et al. 2009; Herath et al. 2014). Maybe also due to the highly sensitive research context, the sample size is similar to other studies in IS compliance research (Hu et al. 2012; Ifinedo 2012).

Table 2. Sample demographics

Variable		Frequency	Percent
Gender	Female	51	52.6
	Male	46	47.4
Age (years)	<= 20	0	0
	21-30	11	12.4
	31-40	31	32.0
	41-50	35	35.1
	51-60	18	18.6
	>= 61	2	2.1
Job tenure (years)	<= 10	17	17.5
	11-20	33	34.0
	21-30	34	35.1
	>= 31	13	13.4
Organizational tenure (years)	<= 10	35	36.1
	11-20	33	34.0
	21-30	20	20.6
	>= 31	9	9.3

Statistical methods

For data analysis, we used partial least squares structural equation modeling (PLS-SEM), which is recommended for the estimation of complex models, including many latent constructs with inner model relationships (Lowry and Gaskin 2014; Wold 1982). PLS-SEM has enjoyed increasing consideration as a key multivariate analysis method (Ringle et al. 2005b). The statistical properties of PLS-SEM in terms of allowing small sample sizes and making no assumptions about the data together with its efficiency and good level of support for predictive and exploratory purposes (Hair et al. 2014) were important reasons for its application. We used the software packages, SmartPLS version 3.0 (Ringle et al. 2005b) and SPSS version 20, for further statistics (e.g. Harman's single-factor test). The bootstrap re-sampling procedure with 5,000 subsamples was used to test the significance of all model paths (Gefen et al. 2000).

Results

Contextual background

In 2010 Securebank suffered from several ISP violations committed by employees, which led to substantial information security incidents. External pressure due to the regulation Basel II was a further reason for strengthening the formal internal controls by using informal controls to establish an appropriate security culture and reduce IS incidents. The bank decided to implement IS awareness-building efforts to complement their internal control system in the same year, and started with developing and distributing conventional materials such as leaflets and posters. Within the last years, their ISA building efforts became more sophisticated, resulting in a variety of materials offered to employees via several internal channels. These internal channels covered online media to distribute electronic articles and e-learning modules on information security. The bank also offered internal security trainings, which were mostly integrated in compliance courses, and provided conventional security materials such as leaflets, cups, and posters, which were handed out to employees at various occasions. It is worth noting that security managers also tried to engage in and promote informal talks about information security to stimulate informal learning between employees. We assessed this situation through interviews (see Table 1) and the study of internal materials. The final interactive presentations with security managers allowed us to reflect on results. Interestingly, the bank perceived the survey conducted in research stage 2 itself as a good intervention to raise ISA and evaluated all recommendations positively. The distribution and assessment of the questionnaire has stimulated the reflection on critical variables, such as personal attitudes, social norms, and neutralization techniques.

Test of the quantitative measurement model

The reflectively measured constructs in the survey were tested using the goodness-of-fit criteria currently recommended by PLS-SEM literature (Cenfetelli et al. 2013; Hair et al. 2014; Hair et al. 2011; Sarstedt et al. 2011). The results show that all of the measures were valid and reliable (see Table 3).

Internal consistency was examined by considering Cronbach's α and composite reliability. Cronbach's α is the lower bound, and composite reliability is the upper bound of the true internal consistency reliability. The values of Cronbach's α and of composite reliability are well above the required value of 0.70, suggesting the measurement model's internal consistency. To accept the criteria of indicator reliability, the outer loadings should be larger than 0.70. All indicators fulfill this requirement, and no indicator had to be dropped. The convergent validity is measured by the average variance extracted (AVE), which should be greater than the required value of 0.5. This requirement is met for each construct. Discriminant validity has also been assessed by checking the cross loadings of the items, which also are acceptable (Hair et al. 2011).

Table 3. Reflective measurement model validity and reliability

Latent Variable	Indicators	Loadings	Cronbach's α	Composite Reliability	AVE
Attitude	ATT1	0.858	0.827	0.897	0.744
	ATT2	0.897			
	ATT3	0.832			
Social norms	SN1	0.920	0.875	0.923	0.801
	SN2	0.838			
	SN3	0.924			
Intention for compliant information security behavior	ICSB1	0.883	0.884	0.928	0.811
	ICSB2	0.891			
	ICSB3	0.927			
Actual compliant information security behavior	CSB1	0.899	0.856	0.913	0.777
	CSB2	0.841			

	CSB3	0.903			
Information security awareness	ISA1	0.872	0.877	0.924	0.802
	ISA2	0.899			
	ISA3	0.916			

The first step in the validation of formative constructs is to check for content validity (Hair et al. 2014). By drawing on context data and closely related studies, we ensured that all formative indicators capture the major facets of the constructs: "internal channel use", "external channel use", and "neutralization techniques" (Bauer et al. 2013a; Craig and Allen 2013; Siponen and Vance 2010). Next, we assessed the level of multicollinearity among indicators, which could cause non-significant weights and problems with the interpretation of the results (e.g. in terms of which items have more or less influence). The assessed variance inflation indicators (VIF) of the indicators for all three constructs can be seen from Table 4, and they are all below the recommended threshold of 5, except for the item "Denial of injury". Hence, we removed this item from the model because the remaining three items still sufficiently capture the construct's content and re-run the analysis without observing critical multicollinearity issues.

Table 4. Weights and VIFs for formative research constructs

Latent Variable	Indicators		Weights	VIF
Internal channel use for information acquisition	ICU1	Online media	0.613	1.488
	ICU2	Trainings	0.110	1.496
	ICU3	Conventional security campaigns	0.348	1.546
	ICU4	Informal talks (colleagues)	0.184	1.503
External channel use for information acquisition	ECU1	Online media	-0.021	1.625
	ECU2	Classic media	0.368	1.556
	ECU3	Self-organized learning	0.778	1.384
	ECU4	Informal talks (family and friends)	0.076	1.559
Neutralization techniques	NEU1	Denial of responsibility	-0.146 (-0.151)	1.612 (1.532)
	NEU2	Condemnation of the condemners	0.648 (0.626)	3.724 (2.513)
	NEU3*	Denial of injury*	-0.044	5.166
	NEU4	Defense of necessity	0.544 (0.527)	3.245 (2.462)

*Dropped due to multicollinearity issues (VIF > 5); Weights and VIF after dropping NEU1 and NEU3 in ( ).

Next, the significance and relevance of the formative indicators is examined through t-statistics (Hair et al. 2014). Out of the twelve indicators of the three formatively measured constructs, the t-values of six indicators are not significant. The next step is to analyze their outer loadings, which are above the threshold of 0.5 for all indicators except for "denial of responsibility". However, the outer loading of this indicator is only marginally below 0.5 (0.49) and significant ($p<.05$), which are conditions suggesting to keep the indicator in the model (Hair et al. 2014). Moreover, the interviews provide support for keeping this indicator of neutralization techniques. Thus, following PLS-SEM recommendations (Cenfetelli and Bassellier 2009; Hair et al. 2014), we retained all indicators in the formative constructs.

Test of the structural model

The structural model was tested with a range of different measures (Hair et al. 2011; Ringle et al. 2005b; Sarstedt et al. 2011). Figure 2 shows the research model together with the main results, including the standardized path coefficients and R^2 values representing the amount of variance in the endogenous construct, as explained by all of the exogenous constructs linked to it. The achieved levels of R^2 in the dependent

variables (ICSB, CSB) are satisfactory when compared to related behavioral research in the ISP compliance area (Bulgurcu et al. 2010; Herath and Rao 2009a; Herath and Rao 2009b; Siponen and Vance 2010; Sommestad and Hallberg 2013). Table 5 extends these results by also including the t-values, effect sizes (f2) and the strengths of these effects, along with final verdicts for each of the underlying research hypotheses. We used the results from bootstrapping with 5,000 subsamples as a non-parametric re-sampling procedure for calculating t-statistics and standard errors (Chin 1998).

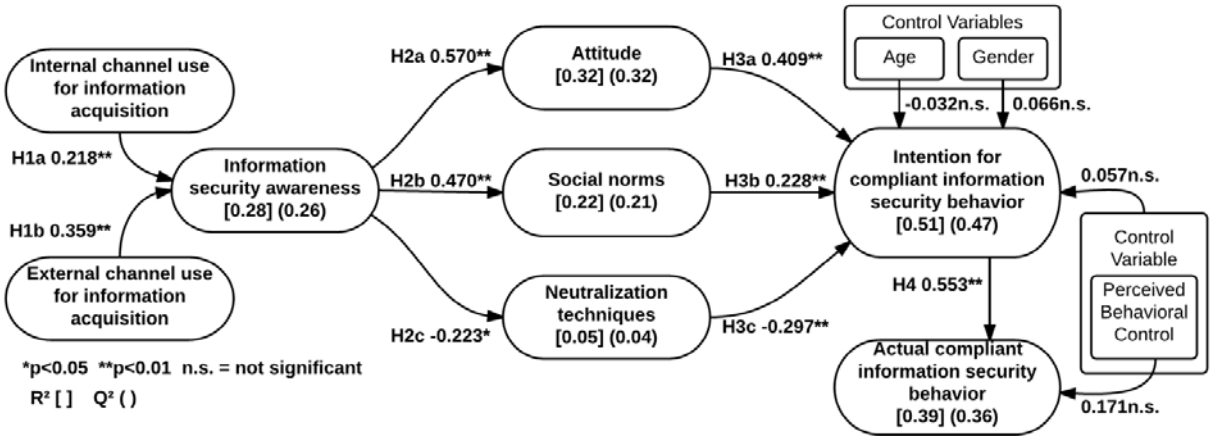


Figure 6. Structural model results

The t-statistics in Table 5 show that all nine hypotheses were supported by the data. The effects of these nine relationships were further analyzed with effect sizes (f2). The effect size f^2 is a standardized statistical measure, which quantifies the relative effect of an exogenous construct on an endogenous construct (Sarstedt et al. 2011). The effect size f2 of a latent factor results from analyzing the decrease in R2 when excluding one independent latent factor. It was suggested that f2 values of .02, .15, and .35 signify small, medium, and large effects, respectively. The next section proceeds with a discussion of each of these effects.

Table 5. Verdict on structural relationships

Hypotheses	Path coefficient	t-values	f^2	Verdict (based on f^2)
H1a: ISA is positively affected by internal channel use for information acquisition.	0.218**	2.928	0.038	weak
H1b: ISA is positively affected by external channel use for information acquisition.	0.359**	4.561	0.102	weak
H2a: ISA has a positive effect on attitude.	0.570**	5.843	0.480	strong
H2b: ISA has a positive effect on social norms.	0.470**	5.145	0.283	moderate
H2c: ISA has a negative effect on neutralization techniques.	-0.223*	2.458	0.052	weak
H3a: Attitude has a positive effect on intention for compliant information security behavior.	0.409**	3.943	0.274	moderate
H3b: Social norm has a positive effect on intention for compliant information security behavior.	0.228**	2.562	0.073	weak
H3c: Neutralization techniques have a negative effect on intention for compliant information security behavior.	-0.297**	3.274	0.161	weak
H4: Intention for compliant information security behavior has a positive effect on the actual compliant information security behavior.	0.553**	4.712	0.455	strong

*p<0.05; **p<0.01

Mediation analysis

Next, we test for the conditions and significance of the potential indirect effects of ISA on the intention for compliant information security behavior considering attitudes, neutralization techniques, and social norms as potential mediators. We adopted Baron and Kenny's causal multi-step mediation test (Baron and Kenny 1986) as follows. First, we assessed the significance of the indirect variable for predicting the mediators. Second, the mediators should affect the behavioral intentions. Both steps are fulfilled for all three cases, which we already established in the previous subsection. Third, we added a direct path between the indirect variable and behavioral intentions, which proved to be significant ($\beta=0.312$, $p<0.01$). When removing one of the mediators and recalculating the PLS-SEM, the path coefficient on this direct path increases and remained significant. Finally, we tested the significance of the indirect effects by performing bootstrapping with replacement (Shrout and Bolger 2002) and the Sobel test (Sobel 1982). Based on this analysis, we report that the positive effects of ISA are partially mediated by attitudes ($p<0.01$), neutralization techniques ($p<0.05$) and social norms ($p<0.05$).

Discussion, implications, and future research

This theory testing single case study provides a theoretically driven explanation that accounts for compliant information security behavior at an international bank. Besides collecting context data through interviews, interactive presentations, and studying internal materials, we conducted a quantitative study based on PLS-SEM (Lowry and Gaskin 2014) to test the developed research hypotheses. Within the scope and boundaries of our case, our findings highlight an ISA to the reasoned compliant action model including the use of information channels for information acquisition, attitudes, and different norms. The study offers three main areas of theoretical and practical implications, which we will now discuss before acknowledging its limitations.

The role of channel use for information acquisition

This study investigates how ISA is fostered through the use of internal and external channels to acquire information and thereby offers specific practical implications in terms of designing ISA programs and establishing input-oriented metrics for measuring ISP compliance. Support was found for the relevance of both the individual utilization of internal and external channels for information acquisition (weak positive effects), which confirms hypotheses 1a-b. While this finding is consistent with previous research generally suggesting that information processing is a precondition for changing behavior (Campbell 1963; Fishbein and Ajzen 1975), we specifically report on the effectiveness of internal and external channel use for information acquisition within the theoretical framework applied to our case study. Through the interviews, we were able to specifically target four internal channels, which the bank exploits to increase ISA among employees. Based on the calculated outer weights, design practices for ISA programs should prioritize internal online channels, including e-learning or intranet messages, together with conventional security campaigns covering internal newspapers, posters, and leaflets when educating users on information security. Relatively less important are trainings and informal channels such as talks with coworkers to raise ISA. Additionally, external information channels to acquire information also contribute to ISA building. In the external domain, self-organized learning is clearly most important. Also traditional media such as newspapers, TV, and radio contribute to ISA. However, talks with family and friends and the use of external online sources such as videos on YouTube or massive, open online courses are relatively less important. In comparison, the use of external channels has an even stronger effect on ISA than internal channels. As another implication to practice, the bank should allow and actively promote and integrate the use of external information sources and self-directed learning in their ISA programs (e.g. by providing a weekly media digest pointing to further external sources on information security incidents worldwide). Considering these findings and the possibility to translate individual knowledge into a ISP compliance metric (Pahnila et al. 2013b), business practice should systematically track both the provision and consumption of information based on various sources and media, which can be seen as leading or input-oriented metrics of ISP compliance.

The role of information security awareness (ISA)

Support was also found for the relevance of ISA in influencing all three postulated predecessors of intention for compliant behavior including attitudes, social norms, and the use of neutralization techniques as a

reflection of personal moral norms. As ISA reflects IS related knowledge, we conceptualized ISA as employees' cognitive ability to recognize their information security mission in the bank. Our results show that ISA not only significantly impacts attitudes toward ISP compliance (strong positive effects), but also the perceived social norm (moderate positive effects), and to a lesser extent neutralization techniques (weak negative effects), thereby confirming hypotheses 2a-c. The mediation analysis further shows that the effects of ISA on the intention for compliant IS behavior are partially mediated by all three constructs, with attitudes exhibiting the relatively strongest mediation effects. These results add to previous research on organizational interventions such as ISA programs for improving employees' ISP compliance (Albrechtsen and Hovden 2010; Eminağaoğlu et al. 2009; Hagen et al. 2011) by confirming the importance of ISA. Moreover, we add empirical evidence to conceptual studies on the importance of ISA, which do not specifically test postulated relationships between ISA and certain predecessors of the intended behavior (Siponen 2000; Thomson and von Solms 1998).

The roles of attitudes and norms

The results show that improvements of attitudes, and personal and social norms are related with an increased intention for compliant information security behavior, thereby confirming hypotheses 3a-c. Our results and integrated analysis, in particular, extend previous work, focusing either on personal norms (Li et al. 2010) or social norms (Herath and Rao 2009a; Herath and Rao 2009b). The intention to comply was confirmed as a strong predictor of actual compliant information security behavior, confirming hypothesis 4.

The results demonstrate that employees' personal moral norms are of essential importance for a compliant information security behavior. More specifically, we add to prior research emphasizing the importance of personal norms (Li et al. 2010) by showing that the use of neutralization techniques has a weak negative effect on the intention for compliant information security behavior, thereby limiting the banks' efforts for establishing information security compliance (Cox 2012). Consistent with prior research, we therefore find that our neutralization construct is a clear predictor of an employee's intention to comply (Siponen and Vance 2010). In combination with the view that security communication and training can effectively focus on neutralization techniques (Barlow et al. 2013), we therefore suggest to practice to also incorporate information on unwanted neutralization in ISA programs. More specifically, the neutralization techniques "condemnation of the condemners" and "defense of necessity" require special attention in our case organization, as these are relatively more important than "denial of injury" and "denial of responsibility" according to our quantitative analysis. This finding is consistent with Barlow's et al. (2013) recommendations, who have also established that certain techniques of neutralization are more powerful than others depending on the given organizational context. As a practical implication regarding "condemnation of the condemners", security managers should only introduce ISP which are perceived as reasonable and fair. In terms of "defense of necessity", employees could be reminded that urgent work and deadlines are no valid justifications for ignoring the ISP. As prior research reported that the perceived detection probability significantly increases the compliance intention when personal norms are relatively weak (Li et al. 2010), we recommend that ISA programs should also make users aware of the possibility of detection, possibly by highlighting the formal controls related to monitoring (Bauer and Bernroider 2015). Building on Li et al. (2010), this should reduce the negative effects of any neutralization techniques.

The weak positive effects of social norms on the intention for a compliant behavior provide empirical evidence for the importance of the social environment (Herath and Rao 2009a; Herath and Rao 2009b). This finding provides an important insight for security managers, who could proactively work on social norms and foster security cultures (Hu et al. 2012; Van Niekerk and Von Solms 2010) by appointing ambassadors of security among employees (Guo 2013). A strong security culture is likely to pressure employees to comply with the ISP (Herath and Rao 2009a; Merhi and Midha 2012) and could be generally enhanced by more actively involving employees in banks' ISA programs (Albrechtsen and Hovden 2010; Van Niekerk and Von Solms 2010).

We contribute to existing literature either highlighting personal norms (Li et al. 2010) or social norms (Herath and Rao 2009a; Herath and Rao 2009b) by integrating both norms in one model. In relative terms, neutralization techniques, the employees' personal norms, were identified as being slightly more important than social norms. Due to the significance of personal norms, we suggest that future research may also investigate whether personality types as recently considered in related behavioral information security

context (Kajzer et al. 2014) constrain or strengthen the identified relationship between ISA and employees' personal moral norms.

However, most important in relative terms are the attitudes toward ISP compliance that should eventually propagate into higher levels of compliant information security behavior. This finding is consistent with Siponen et al. (2014c, but it contradicts previous studies on TRA/TPB in the behavioral information security compliance context, which reported that other constructs have similar or stronger effects than attitudes (Bulgurcu et al. 2010; Herath and Rao 2009b; Hu et al. 2012). A possible explanation refers to the context of SecureBank in relation to these studies using student (Hu et al. 2012) and mixed professional (Bulgurcu et al. 2010; Herath and Rao 2009b) samples. We assume that the attitude-behavior link is stronger when the participating respondents are real employees attributing a higher value to performing the behavior, especially in the banking industry context. As a practical implication, ISA programs should emphasize positive frames and the value for the organization gained by compliant IS behavior instead of overly stressing sanctions (Siponen and Vance 2010). Allowing well-informed employees to understand the benefits of following ISP will further strengthen their attitudes according to our previous theoretical (Baranowski et al. 2003; Chaffee and Roser 1986; Khan et al. 2011; Parsons et al. 2014) and empirical reasoning.

Limitations and future research

Finally, we need to acknowledge limitations that also point to future research. As a start, our results directly apply to the headquarters of the considered international bank. Therefore, in terms of external validity, we offer suggestions based on analytical generalization only. Our study should be replicated to strengthen the support for our findings. Any inferences made to other organizations, particularly outside of our study's contextual domain, should be treated with caution. As we could not implement any forms of experimental control as part of our quantitative data collection, we could not empirically test the causal ordering of the hypothesized relationships. Future studies could introduce experimentation or longitudinal research to overcome this limitation. Another limitation is the use of an online survey distributed through the intranet homepage and e-mails to all headquarter employees. For quality control, we used the IP addresses of respondents to ensure that the right targets participated. We used self-reported data, a common approach in the field of behavioral information security compliance that was used in closely related studies (Bulgurcu et al. 2010; Ifinedo 2014; Siponen et al. 2014c). Finally, the use of a mono-method in the survey, which is common to many studies of similar design, such as that of Fink and Neumann (2009, may have introduced certain levels of common method variance, which we tested and classified as low. As another reliability measure, our latent-variable structuring approach required multiple operationalizations of each construct, which is seen to be more reliable than single-indicator measurements (Baron and Kenny 1986). As overly long surveys are likely to result in respondent fatigue, decreased response rates, and increased missing values (Hair et al. 2014), we in particular implemented the "neutralization techniques" construct with less items compared to prior research (Siponen and Vance 2010). However, to preserve content validity, we developed the construct based on both interview data and prior studies.

Conclusions

The enabling role of internal and external channel use for facilitating ISA in banking organizations is an insufficiently considered question in information systems research. In this quantitative case study based on an employee survey, we applied a new theoretical model integrating information security awareness (ISA), the theory of reasoned action (TRA), and extended norms to understand how compliant information security behavior in a large bank emerges from employees' channel use. The empirical findings clearly support the proposed research model and suggest that for the case organization, leveraging security information, particularly from external sources, fosters ISA, which impacts all considered predictors of the intention for compliant information security behavior and actual compliant information security behavior. Rather than advocate a direct link between awareness and behavior, we suggest a more nuanced approach that focuses on how improved employee awareness gained from channel use not only reduces unwanted neutralization techniques, but also increases the levels of well-accepted predictors of reasoned action in terms of compliance. Out of these predictors, the results demonstrate that the attitude toward ISP compliance is the most important variable followed by both social and personal norms, in the end influencing compliant information security behavior. The regularly overlooked importance of personal norms, here considered as neutralization techniques, which need to be reduced to foster compliance, is supported in our research model.

Therefore, our findings add to the extant literature by explaining how compliant employee behavior in banks develops from attitudes and extended norms, including neutralization considerations. Moreover, we offer important insights into banking practice, as banks continue to struggle with information security-related operational risks despite demanding regulatory requirements. In this regard, our findings provide specific managerial implications for reducing information security risks related to non-compliant employee information security behavior. For example, we provide evidence that specific internal and external channel use should be utilized to improve ISA, which is a central background factor for ultimately tightening information security in banks through attitudes as well as social and personal norms.

References

Abawajy, J. (2012). "User preference of cyber security awareness delivery methods". *Behaviour & Information Technology*, Vo. 33, No. 3: pp. 237-248.

Abu-Musa, A. A. (2006). "Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry". *Journal of Information Systems*, Vo. 20, No. 1: pp. 187-203.

Ajzen, I. (1985). "From intentions to actions: A theory of planned behavior". Heidelberg: Springer *Action-control: From cognition to behavior* pp. 11-39.

Ajzen, I. (1991). "The theory of planned behavior". *Organizational Behavior and Human Decision Processes*, Vo. 50, No. 2: pp. 179-211.

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

Allport, G. W. (1935). "Attitudes". Worcester, MA: Clark University Press *Handbook of social psychology* pp. 798-844.

Armitage, C. J., & Conner, M. (2001). "Efficacy of the Theory of Planned Behavior: A meta-analytic review". *British Journal of Social Psychology*, Vo. 40, pp. 471-499.

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). "Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts?". *Obesity Research*, Vo. 11, No. S10: pp. 23-43.

Barclay, D., Higgins, C., & Thompson, R. (1995). "The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration". *Technology studies*, Vo. 2, No. 2: pp. 285-309.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). "Don't make excuses! Discouraging neutralization to reduce IT policy violation". *Computers & Security*, Vo. 39, pp. 145-159.

Baron, R. M., & Kenny, D. A. (1986). "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations". *Journal of Personality and Social Psychology*, Vo. 51, No. 6: pp. 1173-1182.

Bauer, S., & Bernroider, E. W. N. (2013). "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from exploratory Case Study". *Proceedings of the International Conference Information Systems 2013*, Lissabon. pp. 30-38.

Bauer, S., & Bernroider, E. W. N. (2015). "The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring": Springer International Publishing *Human Aspects of Information Security, Privacy, and Trust* Vol. 9190, pp. 154-164.

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2013). "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study". *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security". *European Journal of Information Systems*, Vo. 18, No. 2: pp. 151-164.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness". *MIS Quarterly*, Vo. 34, No. 3: pp. 523-548.

Campbell, D. T. (1963). "Social attitudes and other acquired behavioral dispositions". New York: McGraw-Hill *Psychology: A study of a science* Vol. 6, pp. 94-172.

Cenfetelli, R. T., & Bassellier, G. (2009). "Interpretation of Formative Measurement in Information Systems Research". *MIS Quarterly*, Vo. 33, No. 4: pp. 689-707.

Cenfetelli, R. T., Bassellier, G., & Posey, C. (2013). "The Analysis of Formative Measurement in IS Research: Choosing between Component- and Covariance-based Techniques". *The DATA BASE for Advances in Information Systems*, Vo. 44, No. 4: pp. 66-79.

Chaffee, S. H., & Roser, C. (1986). "Involvement and the Consistency of Knowledge, Attitudes, and Behaviors". *Communication Research*, Vo. 13, No. 3: pp. 373-399.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). "Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory". *Computers in Human Behavior*, Vo. 38, pp. 220-228.

Chin, W. W. (1998). "The Partial Least Squares Approach to Structural Equation Modeling". New Jersey: Lawrence Erlbaum Associates *Modern Methods for Business Research* Vol. 8, pp. 295-336.

Ciborra, C. (2006). "Imbrication of Representations: Risk and Digital Technologies". *The Journal of Management Studies*, Vo. 43, No. 6: pp. 1339-1356.

Connelly, C. E., Archer, N. P., Yuan, Y., & Guo, K. H. (2011). "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model". *Journal of Management Information Systems*, Vo. 28, No. 2: pp. 203-236.

Cox, J. (2012). "Information systems user security: A structured model of the knowing–doing gap". *Computers in Human Behavior*, Vo. 28, No. 5: pp. 1849-1858.

Craig, A. C., & Allen, W. M. (2013). "Sustainability information sources: employee knowledge, perceptions, and learning". *Journal of Communication Management*, Vo. 17, No. 4: pp. 292-307.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). "Future directions for behavioral information security research". *Computers & Security*, Vo. 32, pp. 90-101.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach". *Information Systems Research*, Vo. 20, No. 1: pp. 79-98.

Davidson, A. R., Yantis, S., Norwood, M., & Montano, D. E. (1985). "Amount of information about the attitude object and attitude–behavior consistency". *Journal of Personality and Social Psychology*, Vo. 49, No. 5: pp. 1184-1198.

Dhillon, G. (1999). "Managing and controlling computer misuse". *Information Management & Computer Security*, Vo. 7, No. 4: pp. 171-175.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). "User behaviour towards protective information technologies: the role of national cultural differences". *Information Systems Journal*, Vo. 19, No. 4: pp. 391-412.

Donovan, R. (2011). "Theoretical models of behaviour change". *The SAGE Handbook of Social Marketing* pp. 15-31.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research". *Academy of Management Review*, Vo. 14, No. 4: pp. 532-550.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). "The positive outcomes of information security awareness training in companies – A case study". *Information Security Technical Report*, Vo. 14, No. 4: pp. 223-229.

Fabrigar, L. R., Petty, R. E., Smith, S. M., & Crites Jr, S. L. (2006). "Understanding knowledge effects on attitude-behavior consistency: The role of relevance, complexity, and amount of knowledge". *Journal of Personality and Social Psychology*, Vo. 90, No. 4: pp. 556-577.

Fink, L., & Neumann, S. (2009). "Exploring the perceived business value of the flexibility enabled by information technology infrastructure". *Information & Management*, Vo. 46, No. 2: pp. 90-99.

Fishbein, M. (2000). "The role of theory in HIV prevention". *AIDS care*, Vo. 12, No. 3: pp. 273-278.

Fishbein, M., & Ajzen, I. (1975). "*Belief, attitude, intention and behavior"*. Reading, MA: Addison-Wesley.

Fishbein, M., & Ajzen, I. (2010). "*Predicting and Changing Behavior: The Reasoned Action Approach"*: Psychology Press, Taylor & Francis Group.

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). "Structural Equation Modeling and Regression: Guidelines for research practice". *Communications of the Association for Information Systems*, Vo. 4, No. 7: pp. 1-79.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories". *Journal of the Association for Informaton Systems*, Vo. 12, No. 9: pp. 606-631.

Guo, K. H. (2013). "Security-related behavior in using information systems in the workplace: A review and synthesis". *Computers & Security*, Vo. 32, pp. 242-251.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). "Understanding nonmalicious security violations in the workplace: a composite behavior model". *Journal of Management Information Systems*, Vo. 28, No. 2: pp. 203-236.

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). "The long-term effects of information security e-learning on organizational learning". *Information Management & Computer Security*, Vo. 19, No. 3: pp. 140-154.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). "Implementation and effectiveness of organizational information security measures". *Information Management & Computer Security*, Vo. 16, No. 4: pp. 377-397.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). "*A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)"*. Thousand Oaks: SAGE Publications Ltd.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2011). "An assessment of the use of partial least squares structural equation modeling in marketing research". *Journal of the Academy of Marketing Science*, Vo. 40, No. 3: pp. 414-433.

Harrington, S. J. (1996). "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions". *MIS Quarterly*, Vo. 20, No. 3: pp. 257-278.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service". *Information Systems Journal*, Vo. 24, No. 1: pp. 61-84.

Herath, T., & Rao, H. R. (2009a). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness". *Decision Support Systems*, Vo. 47, No. 2: pp. 154-165.

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

Hsu, C., Backhouse, J., & Silva, L. (2013). "Institutionalizing operational risk management: an empirical study". *Journal of Information Technology*, Vo. 29, No. 1: pp. 59-72.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture". *Decision Sciences,* Vo. 43, No. 4: pp. 615-659.

Ifinedo, P. (2012). "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory". *Computers & Security,* Vo. 31, No. 1: pp. 83-95.

Ifinedo, P. (2014). "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition". *Information & Management,* Vo. 51, No. 1: pp. 69-79.

Im, G. P., & Baskerville, R. (2005). "A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error". *The DATA BASE for Advances in Information Systems,* Vo. 36, No. 4: pp. 68-79.

Johnston, A. C., & Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study". *MIS Quarterly,* Vo. 34, No. 3: pp. 549-566.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). "An exploratory investigation of message-person congruence in information security awareness campaigns". *Computers & Security,* Vo. 43, pp. 64-76.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). "Effectiveness of information security awareness methods based on psychological theories". *African Journal of Business Management,* Vo. 5, No. 26: pp. 10862-10868.

Lanier, M., Henry, S., & Desire'JM, A. (2004). "*Essential Criminology"* (4 ed.). Boulder: Perseus Books Group.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). "Information Security Awareness and Behavior: a theory-based literature review". *Management Research Review,* Vo. 37, No. 12: pp. 1049-1092.

Li, H., Zhang, J., & Sarathy, R. (2010). "Understanding compliance with internet use policy from the perspective of rational choice theory". *Decision Support Systems,* Vo. 48, No. 4: pp. 635-645.

Lim, V. K. G. (2002). "The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice". *Journal of Organizational Behavior,* Vo. 23, No. 5: pp. 675-694.

Liu, Q., & Vasarhelyi, M. (2014). "Big Questions in AIS Research: Measurement, Information Processing, Data Analysis, and Reporting". *Journal of Information Systems,* Vo. 28, No. 1: pp. 1-17.

Lowry, P. B., & Gaskin, J. (2014). "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It". *IEEE Transactions on Professional Communication,* Vo. 57, No. 2: pp. 123-146.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). "Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research". *Management Science,* Vo. 52, No. 12: pp. 1865-1883.

Maruna, S., & Copes, H. (2005). "What Have We Learned from Five Decades of Neutralization Research?". *Crime and Justice,* Vo. 32, pp. 221-320.

Merhi, M. I., & Midha, V. (2012). "The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study". *Proceedings of the International Conference on Information Systems (ICIS),* Orlando. pp. 1-11.

Minor, W. W. (1981). "Techniques of neutralization: A reconceptualization and empirical examination". *Journal of Research in Crime and Delinquency,* Vo. 18, No. 2: pp. 295-318.

Modell, S. (2005). "Triangulation between case study and survey methods in management accounting research: An assessment of validity implications". *Management Accounting Research,* Vo. 16, No. 2: pp. 231-254.

Moore, D. L., & Tarnai, J. (2002). "Evaluating nonresponse error in mail surveys". New York: John Wiley & Sons *Survey nonresponse* pp. 197–211.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). "Information Security Behavior: Towards Multi-stage Models". *Proceedings of the Pacific Asia Conference on Information Systems (PACIS),* Jeju Island (Korea).

Pahnila, S., Siponen, M., & Mahmood, M. A. (2007). "Employees' Behavior towards IS Security Policy Compliance". *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS),* Hawaii

Pare, G. (2004). "Investigating information systems with positivist case research". *The Communications of the Association for Information Systems,* Vo. 13, No. 1: pp. 233-264.

Parker, D., Manstead, A. S., & Stradling, S. G. (1995). "Extending the theory of planned behaviour: The role of personal norm". *British Journal of Social Psychology,* Vo. 34, No. 2: pp. 127-138.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)". *Computers & Security,* Vo. 42, pp. 165-176.

Pfleeger, S. L., & Caputo, D. D. (2012). "Leveraging behavioral science to mitigate cyber security risk". *Computers & Security,* Vo. 31, No. 4: pp. 597-611.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies". *Journal of Applied Psychology,* Vo. 88, No. 5: pp. 879-903.

Podsakoff, P. M., & Organ, D. W. (1986). "Self-reports in organizational research: Problems and prospects". *Journal of Management,* Vo., No. 12: pp. 69–82.

PricewaterhouseCoopers. (2014). "Information Security Breaches Survey". *The Department for Business, Innovation and Skills, BIS/14/767*.

Quagliata, K. (2011). Impact of Security Awareness Training Components on Perceived Security Effectiveness. *ISACA Journal [Online Exclusive], 4*. Retrieved from http://www.isaca.org/Journal/archives/2011/Volume-4/Pages/JOnline-Impact-of-Security-Awareness-Training-Components-on-Perceived-Security-Effectiveness.aspx [accessed 31 December 2015]

Riege, A. M. (2003). "Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase". *Qualitative market research: An international journal*, Vo. 6, No. 2: pp. 75-86.

Ringle, C., Wende, S., & Will, A. (2005). SmartPLS 2.0 (beta). Retrieved 12.1.2012, from University of Hamburg http://www.smartpls.de

Rivis, A., & Sheeran, P. (2003). "Descriptive norms as an additional predictor in the theory of planned behaviour: A meta-analysis". *Current Psychology*, Vo. 22, No. 3: pp. 218-233.

Roberts, P., & Henderson, R. (2000). "Information technology acceptance in a sample of government employees: a test of the technology acceptance model". *Interacting with Computers*, Vo. 12, No. 5: pp. 427-443.

Rocha Flores, W., & Antonsen, E. (2013). "The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods". *Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM)*, Natal, Brazil. pp. 1-15.

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2011). "PLS-SEM: Indeed a Silver Bullet". *The Journal of Marketing Theory and Practice*, Vo. 19, No. 2: pp. 139-152.

Shrout, P. E., & Bolger, N. (2002). "Mediation in experimental and nonexperimental studies: New procedures and recommendations". *Psychological Methods*, Vo. 7, No. 4: pp. 422-445.

Siponen, M. (2000). "A conceptual foundation for organizational information security awareness". *Information Management & Computer Security*, Vo. 8, No. 1: pp. 31-41.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). "Employees' adherence to information security policies: An exploratory field study". *Information & Management*, Vo. 51, No. 2: pp. 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). "Compliance with Information Security Policies An Empirical Investigation". *IEEE Computer*, Vo. 43, No. 2: pp. 64-71.

Siponen, M., & Vance, A. (2010). "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations". *MIS Quarterly*, Vo. 34, No. 3: pp. 487-502.

Siponen, M., & Vance, A. (2013). "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations". *European Journal of Information Systems*, Vo. 23, No. 3: pp. 289-305.

Sobel, M. E. (1982). "Asymptotic confidence intervals for indirect effects in structural equation models". Washington DC: American Sociological Association *Sociological Methodology* pp. 290-312.

Sommestad, T., & Hallberg, J. (2013). "A review of the theory of planned behaviour in the context of information security policy compliance". *International Information Security and Privacy Conference*.

Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R., & Samson, D. (2002). "Effective case research in operations management: a process perspective". *Journal of Operations Management*, Vo. 20, No. 5: pp. 419-433.

Sykes, G. M., & Matza, D. (1957). "Techniques of Neutralization: A Theory of Delinquency". *American Sociological Association*, Vo. 22, No. 6: pp. 664-670.

Thomson, M. E., & von Solms, R. (1998). "Information Security Awareness: Educating the Users effectively". *Information Management & Computer Security*, Vo. 6, No. 4: pp. 167-173.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). "Managing the introduction of information security awareness programmes in organisations". *European Journal of Information Systems*, Vo. 24, No. 1: pp. 38-58.

Van der Stede, W. A., Mark Young, S., & Xiaoling Chen, C. (2006). "Doing Management Accounting Survey Research": Elsevier *Handbooks of Management Accounting Research* Vol. Volume 1, pp. 445-478.

Van Niekerk, J. F., & Von Solms, R. (2010). "Information security culture: A management perspective". *Computers & Security*, Vo. 29, No. 4: pp. 476-486.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention". *European Journal of Information Systems*, Vo. 20, No. 3: pp. 267-284.

Warkentin, M., & Willison, R. (2009). "Behavioral and policy issues in information systems security: the insider threat". *European Journal of Information Systems*, Vo. 18, No. 2: pp. 101-105.

White, K. M., Smith, J. R., Terry, D. J., Greenslade, J. H., & McKimmie, B. M. (2009). "Social influence in the theory of planned behaviour: the role of descriptive, injunctive, and ingroup norms". *British Journal of Social Psychology*, Vo. 48, No. 1: pp. 135-158.

Wicker, A. W. (1969). "Attitudes versus actions: The relationship of verbal and overt behavioral responses to attitude objects". *Journal of Social issues*, Vo. 25, No. 4: pp. 41-78.

Willison, R., & Warkentin, M. (2013). "Beyond Deterrrence: An Expanded View of Employee Computer Abuse". *MIS Quarterly*, Vo. 37, No. 1: pp. 1-20.

Wilson, M., & Hash, J. 2003. "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology (NIST) Special Publication 800-50, Gaithersburg.

Wold, H. (1982). "Soft modeling: the basic design and some extensions". Amsterdam: North-Holland *Systems under indirect observations: Causality, structure, prediction. Part 2* pp. 1-54.

Yin, R. K. (2014). "*Case Study Research: Design and Methods"* (5 ed.). Thousand Oaks: Sage Publications, Inc.

Appendix

Table A1. Measurement model

Construct	**Items**		**Adapted from**
Attitude (reflective)	ATT1	I believe that it is beneficial for an organization to establish clear information security policies, practices, and technologies.	(Hu et al. 2012)
	ATT2	I believe that it is useful for an organization to enforce its information security policies, practices, and technologies.	
	ATT3	I believe that it is a good idea for an organization to establish clear information security policies, practices, and technologies.	
Social norms (reflective)	SN1	In our organization, information security is viewed as a collective responsibility.	(Rocha Flores and Antonsen 2013)
	SN2	My colleagues would warn me if they saw me doing something (e.g. using computer, or disposing sensitive information) in an unsecure way.	
	SN3	My colleagues and I share the same ambitions and vision of protecting information assets from being compromised in our organization.	
Intention for compliant information security behavior (reflective)	ICSB1	I intend to comply with information security policies.	(Siponen et al. 2014; Siponen et al. 2010)
	ICSB2	I intend to assist others in complying with information security policies.	
	ICSB3	I intend to recommend that others comply with information security policies.	
Actual compliant information security behavior (reflective)	CSB1	I comply with information security policies (e.g. secure password, clear desk/screen policy, classification and handling of information).	(Siponen et al. 2014; Siponen et al. 2010)
	CSB2	I assist others in complying with information security policies.	
	CSB3	I recommend that others comply with information security policies.	
Neutralization techniques (formative)	NEU1	It is OK to violate the company information security policy if you don't understand it.	(Siponen and Vance 2010)
	NEU2	It is not wrong to violate a company information security policy, which is not reasonable.	
	NEU3	It is OK to violate the company information security policy if no damage is done to the company.	
	NEU4	It is all right to violate the company information security policy when you are under a tight deadline.	
Internal channel use for information acquisition (formative)		How often do you use internal sources to inform yourself about information security?	(Bauer et al. 2013a)
	ICU1	Online media (E-learning, Intranet to read the security standards)	
	ICU2	Trainings (e.g. seminars, fairs)	
	ICU3	Conventional security campaigns (e.g. posters, flyers, folders)	
	ICU4	Informal talks with colleagues	
External channel use for information		How often do you use external sources to inform yourself about information security?	(Craig and Allen 2013)
	ECU1	Online media (e.g. YouTube videos, online newspapers, E-learning [Mooc's], blogs)	

acquisition (formative)	ECU2	Classic media (e.g. newspaper, TV, radio)	
	ECU3	Self-organized learning (books, articles)	
	ECU4	Informal talks with family and friends	
Information security awareness (reflective)	ISA1	In each work situation I am aware of the information security issues that can be caused or allowed for through my actions as well as eventual negligence.	(Rocha Flores and Antonsen 2013)
	ISA2	I understand concerns regarding information security and the risks that information security threats pose in general.	
	ISA3	I am aware of potential information security threats related to my work and the organization's business activities, as well as the negative consequences they may cause.	

Terms: Information Security Policy (ISP), Information Security (IS)

Scales: All variables (except ICU and ECU) were measured on a scale between strongly disagree (1) and strongly agree (7). ICU and ECU and were measured on a scale between never (1) and very frequently (7).

General theme of survey: At the beginning of the online survey, we clarified that the context of the questions is information security in the organization’s context given by the ISP. Also, the main terms, such as ISP, were introduced to avoid misunderstandings.

Table A2. Fornell-Larcker criterion (only reflective constructs)

	CSB	ATT	ISA	ICSB	SN
Actual compliant information security behavior (CSB)	0.882				
Attitude (ATT)	0.411	0.862			
Information security awareness (ISA)	0.573	0.570	0.896		
Intention for compliant information security behavior (ICSB)	0.605	0.567	0.609	0.901	
Social norms (SN)	0.622	0.357	0.470	0.489	0.895

Table A3. Construct cross loadings (discriminant validity)

	Actual compliant IS behavior (CSB)	Attitude (ATT)	Information security awareness (ISA)	Intention for security compliance behavior (ICSB)	Social norms (SN)
CSB1	0.899	0.359	0.498	0.475	0.508
CSB2	0.841	0.369	0.556	0.518	0.607
CSB3	0.903	0.360	0.463	0.597	0.528
ATT1	0.398	0.858	0.458	0.491	0.313
ATT2	0.377	0.897	0.469	0.478	0.333
ATT3	0.293	0.832	0.540	0.493	0.279
ISA1	0.498	0.451	0.872	0.484	0.339
ISA2	0.481	0.549	0.899	0.596	0.435
ISA3	0.559	0.522	0.916	0.547	0.474
ICSB1	0.419	0.501	0.543	0.883	0.401
ICSB2	0.594	0.509	0.579	0.891	0.516
ICSB3	0.607	0.522	0.527	0.927	0.405
SN1	0.575	0.379	0.471	0.409	0.920
SN2	0.569	0.275	0.336	0.446	0.838
SN3	0.531	0.302	0.446	0.460	0.924

Table A4. Covariance matrix (inner model residual covariance)

	CSB	ATT	ISA	ICSB	ICU	ECU	SN
Actual compliant information security behavior (CSB)	1.000	0.195	-0.036	0.066	0.377	0.258	0.532
Attitude (ATT)	0.195	1.000	-0.271	0.100	0.039	0.028	0.159
Information security awareness (ISA)	-0.036	-0.277	1.000	-0.040	-0.092	-0.125	-0.330
Intention for compliant information security behavior (ICSB)	0.066	0.100	-0.040	1.000	0.186	0.088	-0.009
Internal channel use (ICU)	0.377	0.039	-0.092	0.186	0.159	0.570	0.391
External channel use (ECU)	0.258	0.028	-0.125	0.088	0.570	1.000	0.408
Social norms (SN)	0.532	0.159	-0.330	-0.009	0.391	0.408	1.000

Table A5. Latent variable correlation matrix

	CSB	ATT	ISA	ICSB	ICU	ECU	SN
Actual compliant information security behavior (CSB)	1.000						
Attitude (ATT)	0.411	1.000					
Information security awareness (ISA)	0.573	0.570	1.000				
Intention for compliant information security behavior (ICSB)	0.605	0.567	0.609	1.000			
Internal channel use (ICU)	0.472	0.289	0.454	0.462	1.000		
External channel use (ECU)	0.432	0.301	0.502	0.406	0.655	1.000	
Social norms (SN)	0.622	0.357	0.470	0.489	0.505	0.537	1. 000

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring

Stefan Bauer, Edward W. N. Bernroider

Vienna University of Economics and Business, Austria
Stefan.Bauer,Edward.Bernroider@wu.ac.at

Abstract. Our aim is to understand how information security awareness (ISA) programs affect the intention of employees for compliant information security behavior. We draw on Protection Motivation Theory (PMT) to uncover indirect influences of ISA programs, and seek to identify the extent to which intention translates into actual compliance is contingent on monitoring. Based on partial least squares structural equation modeling analysis of 183 survey responses consisting of German bank employees, we find strong empirical evidence for the importance of ISA programs, protection motivation and monitoring. While ISA programs effectively change how employees cope with and assess security threats, only coping appraisal is an important condition for the positive behavioral effects of such programs to occur. However, ISA programs may cause a false sense of security, as vulnerability perceptions are reduced by consuming ISA programs but not affecting intentions for compliant security behavior. Perceived monitoring strengthens this confirmed intention-behavior link.

Keywords: Information Security Awareness Programs, Protection Motivation Theory, Employee Security Behavior, PLS-SEM, Moderation Effect.

Introduction

Banks' information systems are threatened by a huge variety of risks that arise from employees using information technology in their daily work. Actually, bank industry reports highlight the problematic situation by presenting a total number of 45.050 operational loss events with an average gross loss size of € 285.277 reported by 60 international banking groups (ORX 2014). Incidents associated with the interaction of employees and information systems occur because of a toxic combination of reasons, often related to employees' non-compliance with banks' information security policy (ISP) (Padayachee 2012). Especially for banks, much is at risk, because an information security breach can lead to enormous reputational and operational damages (Goldstein et al. 2011).

To mitigate these risks, banks have implemented employee centric information security awareness (ISA) programs to actively protect their information assets (Bauer et al. 2013b). An increased awareness concerning information security risks and threats is by many considered as the most cost-effective control of an organization (Hagen et al. 2008). ISA programs make employees sensitive to foster security of organizations' information systems and be aware of information security risks (Eminağaoğlu et al. 2009). Actual topics for ISA programs are, among others, phishing attacks, social engineering, passwords security, secure internet use and clear screen policy (Bauer et al. 2013b).

In general, Protection Motivation Theory (PMT) is used to discover motivational influences on the intention for a compliant security behavior (Ifinedo 2012; Rogers 1975). Until now, scientific research has largely neglected analyzing the effects of ISA programs on employees' protection motivation and its subsequent effects on the individual intention to comply with the ISP. We seek to fill this gap and also expect that the variables of PMT will act as mediators governing the relationship between the perception of the ISA programs and the individual's intention to comply with the ISP. Additionally, we assume that employees actually behave in a more desirable way when they know that their actions are monitored by the bank. Previous research on monitoring confirmed that vulnerability or severity may affect individual attitudes toward monitoring (Workman 2009). Hence, we also aim at unraveling the influence on monitoring on the actual behavioral outcomes of these behavioral intentions in the ISP context of our study.

The paper has five sections. The next section provides theoretical foundations of ISA programs and PMT, develops the research hypotheses and the research model. Next, the research methodology is presented followed by the evaluation of the measurement and structural models. Then, we briefly discuss the main findings and finally conclude the paper with a short summary and directions for further research.

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

Research Background and Hypotheses

A recent literature review on behavioral information security research highlights the emphasis of prior research on four major theories, namely Theory of Planned Behavior, General Deterrence Theory, Technology Acceptance Model and the PMT (Lebek et al. 2014). The PMT addresses the determination of fear appeals and how individuals cope with the danger brought about by information security risks and threats (Ifinedo 2012; Rogers 1975). PMT has been considered as one the most powerful theories explaining individuals' intentions to engage in compliant actions (Floyd et al. 2000; Lebek et al. 2014). In the context of information security compliance, prior studies reported positive effects of all constructs of PMT on self-reported behavioral intentions (Lebek et al. 2014; Meso et al. 2013; Siponen et al. 2014b; Workman et al. 2008). Our research aim is to extend these studies by focusing on the evaluation of the impact of ISA programs on employees' protection motivation, which should in turn impact the intention to comply, thereby conceptualizing protection motivation as mediator. Figure 1 visualizes the research model including all hypotheses, which will be developed in the next sub-sections.

The Role of Protection Motivation Theory

PMT has been repeatedly examined and discussed in the extant behavioral information security literature (Herath and Rao 2009a; Herath and Rao 2009b; Ifinedo 2012; Meso et al. 2013; Siponen et al. 2014b; Vance et al. 2012; Workman et al. 2008). The original theory builds upon threat and coping appraisal. Threat appraisal consists of the constructs perceived vulnerability and perceived severity of an event (Siponen et al. 2014b). Perceived vulnerability is defined as an individual's perception of the probability of an information security incident, which in our context is caused by behavioral non-compliance with the ISP (Ifinedo 2012). In contrast, perceived severity reflects the impact of an information security incident caused by non-compliance with the ISP (Ifinedo 2012; Siponen et al. 2010). Previous research has shown mixed results concerning significant effects of perceived vulnerability and perceived severity on intention for compliant security behavior (Herath and Rao 2009b; Ifinedo 2012; Pahnila et al. 2007a; Siponen et al. 2014b). Nonetheless, meta studies showed significant low positive effects (Floyd et al. 2000; Lebek et al. 2014), hence we assume similar outcomes.

Response efficacy and self-efficacy together constitute coping appraisal, which has a significant impact on behavioral intentions according to meta-studies on PMT (Floyd et al. 2000; Milne et al. 2000). Response efficacy is the expectancy of the employee that the threat or risk can be mitigated by conducting the ISP compliant security behavior (Lebek et al. 2014), while self-efficacy is the belief that one is able to conduct the requested behavior for compliance. In particular, self-efficacy has a positive effect on behavioral intention for a compliant security behavior (Ifinedo 2012; Pahnila et al. 2007a; Siponen et al. 2014b). In terms of, response efficacy previous research provides mixed results with no or marginally significant impacts (Johnston and Warkentin 2010; Pahnila et al. 2007a; Siponen et al. 2010) and positive impacts on compliant security behavior (Ifinedo 2012). To conclude, we propose the following:

H1: Perceived vulnerability has a positive effect on the intention for compliant security behavior.
H2: Perceived severity has a positive effect on the intention for compliant security behavior.
H3: Response efficacy has a positive effect on the intention for complaint security behavior.
H4: Self-efficacy has a positive effect on the intention for compliant security behavior.

The Effects of ISA Programs on Employees' Protection Motivation

The aim of ISA programs is to increase employees' ISA concerning current information security threats and risks by delivering the content of the ISP to banks' employees (Bauer et al. 2013b; Tsohou et al. 2013). In practice, ISA programs vary from bank to bank and different methods are used to make their employees more aware (Bauer and Bernroider 2013b; Bauer et al. 2013b). ISA programs can be structured as intense and coordinated campaigns or simply consist of several isolated initiatives (Bauer et al. 2013b; Kajzer et al. 2014). An increased ISA through such programs can lead to improvements of employees' security compliance behavior (Eminağaoğlu et al. 2009). Hence, we generally assume that ISA programs positively affect the intention for compliant security behavior (Bauer and Bernroider 2013a). More specifically, we posit that ISA programs have positive direct and indirect effects on the intention for compliant security behavior. The indirect effects should be delivered via the PMT constructs as mediators. We therefore suggest:

H5 (direct effects): ISA programs have a positive effect on the intention for compliant security behavior.
H5a-d (indirect effects): The positive effects of ISA programs on the intention for compliant security behavior are mediated by perceived vulnerability (H5a), by perceived severity (H5b), by response efficacy (H5c), and by self-efficacy (H5d).

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

ISA programs usually highlight current information systems risks and threats, such as those related to phishing or other social engineering attacks (Bauer et al. 2013b). Consequently, employees should benefit from getting a realistic picture of threat scenarios. Thus, we assume that ISA programs increase employees' perceptions on vulnerabilities and threat severity. Moreover, employees' response efficacy and self-efficacy should benefit from ISA programs, because employees usually also receive more knowledge about rules and work practices and information on how to conduct compliant security behavior (Bauer et al. 2013b). We assume that employees' ISA is an important precondition for employees' protection motivation, hence we propose:

H6: ISA programs have a positive effect on perceived vulnerability.
H7: ISA programs have a positive effect on perceived severity.
H8: ISA programs have a positive effect on response efficacy.
H9: ISA programs have a positive effect on self-efficacy.

The Role of Perceived Monitoring

Behavioral theories basing on self-reported data often examine the relationship between behavioral intent and actual behavior (Lebek et al. 2014). The correlation of these two constructs is assumed in the Theory of Planned Behavior as well as in PMT (Lebek et al. 2014). Hence, a variety of studies have already confirmed the significance of this relationship in behavioral information security context (Pahnila et al. 2007a; Siponen et al. 2014b; Siponen et al. 2010). But recent research calls for more research on the behavioral contingencies of intention, i.e., the variables which possibly moderate the effects of intention on actual behavior (Lebek et al. 2014). Especially in the banking context, money is data in the information systems and banks need to monitor how employees are acting (Bauer et al. 2013b). We assume that the employees' perception of monitoring will enhance his or her actual compliant security behavior. Hence, we conclude:

H10: The intention for compliant security behavior has a positive effect on actual compliant security behavior.
H11: Perceived monitoring has a positive moderation effect on the positive relationship between intention and actual complaint security behavior.

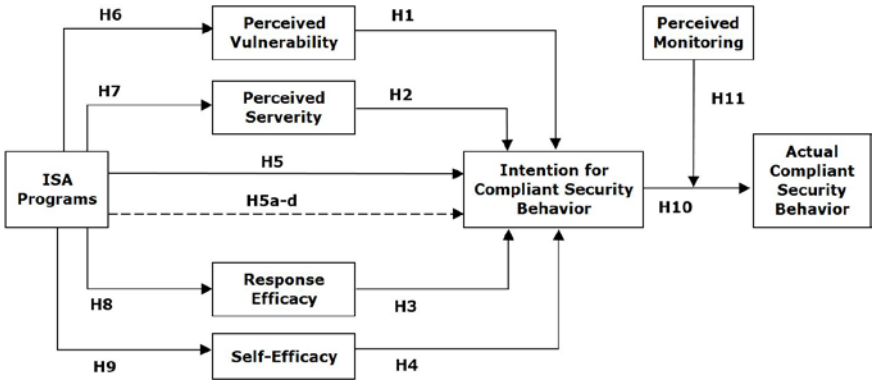


Fig. 7. Research Model and Hypotheses

Research Methodology

A positivistic research approach was applied to test the developed research hypotheses with a quantitative survey. All constructs of our research model were adopted from supporting empirical research in the context of behavioral information security (D'Arcy and Hovav 2008; Hu et al. 2012; Ifinedo 2012; Siponen et al. 2010). The questionnaire was pre-tested and afterwards improved according to pre-testers' comments.

Finally, we utilized a crowdsourcing platform to contact bank employees from German banks. The platform has a user base of 70,000 active members from all regions in Germany, which were all invited to participate. The respondents first had to qualify as valid target persons before they were invited to assess the questionnaire. This multistage selection process finally led to 183 valid responses from bank employees working in Germany and allowed for covering a range of different banks which differ in the frequency and quality of their ISA programs. A recent study suggested that respondents from crowdsourcing platforms have advantages over other sampling procedures commonly used in behavioral survey research. While their response behavior seems to be equal to traditional participants pools, they, e.g., offer more diversity in particular in terms of work experience when compared to student samples (Behrend et al. 2011). However, our sample seems to be biased towards younger male professionals. It consists of 135 men and 48 women,

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

and the majority of the respondents is below 30 years old. 85% of the respondents have between one and ten years work experience in the banking sector.

The collected data was analyzed by conducting a partial least squares structural equation modeling (PLS-SEM) analysis (Hair et al. 2013) with SmartPLS (Ringle et al. 2005a). We carefully considered all quality and validity criteria following current recommendations (Hair et al. 2013; Hair et al. 2011; Sarstedt et al. 2011).

Validation of the Measurement Model

The measurement model was tested with all quality and validity criteria required by contemporary recommendations (Hair et al. 2013; Hair et al. 2011; Sarstedt et al. 2011). Table 1 summarizes the goodness-of-fit criteria. First, all relevant values of Cronbach's α and composite reliability are above the critical value (0.70), which is evidence for internal consistency reliability of the results. Second, all assessed loadings exhibit above the required value of 0.70, hence indicator reliability is adequate. Third, regarding convergent validity, the recommended threshold of 0.50 for the criteria AVE was exceeded by all values, hence more than the half of the variance of the indicators is explained by the constructs (Hair et al. 2013). Overall, all considered quality and validity criteria meet the contemporary recommendations.

Table 3. Measurement model validity and reliability (all constructs are reflective)

Latent Var.	Indicators	Loadings	Cronbach's α	Composite Rel.	AVE
Perceived Vulnerability	PV1	0.88	0.85	0.91	0.77
	PV2	0.86			
	PV3	0.88			
Perceived Severity	PS1	0.90	0.85	0.91	0.76
	PS2	0.83			
	PS3	0.88			
Response efficacy	RE1	0.93	0.81	0.91	0.84
	RE2	0.91			
Self-efficacy	SE1	0.89	0.86	0.91	0.77
	SE2	0.92			
	SE3	0.83			
ISA program	ISAP1	0.83	0.70	0.83	0.63
	ISAP2	0.81			
	ISAP3	0.73			
Intention for Compliant Sec. Behavior	ICSB1	0.85	0.79	0.88	0.71
	ICSB2	0.84			
	ICSB3	0.83			
Perceived Monitoring	PM1	0.85	0.79	0.87	0.70
	PM2	0.77			
	PM3	0.88			
Actual Compliant Sec. Behavior	AP1	0.85	0.73	0.84	0.64
	AP2	0.83			
	AP3	0.72			

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

Evaluation of the Structural Model

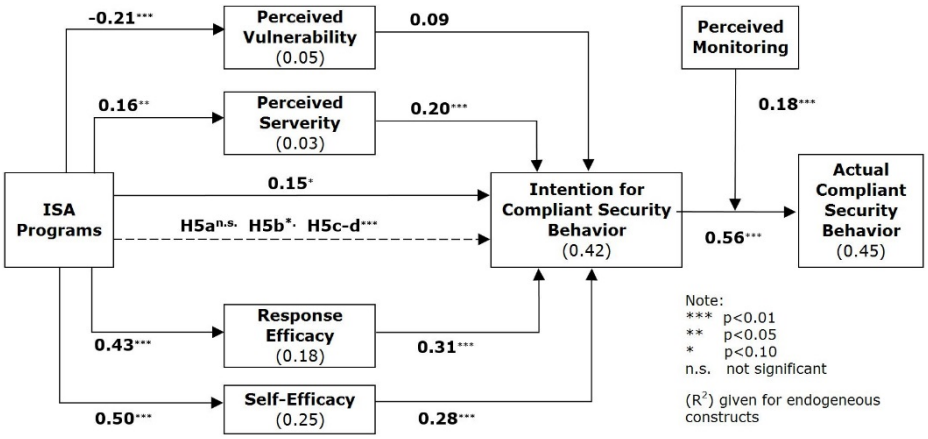


Fig. 8. Empirical Results

We firstly conducted a PLS-SEM analysis to test the direct effects of PMT's latent constructs and examine the proposed hypotheses. As Figure 2 illustrates, the research models' predictive accuracy for the variables intention for compliant security behavior and actual compliant security behavior seems to be acceptable, because the values of R^2 are high compared with the results of prior research (Lebek et al. 2014; Siponen et al. 2014b) and recommendations from scholarly research (Hair et al. 2013). In contrast, R^2 values of perceived vulnerability and perceived severity are low. Furthermore, the achieved level of R^2 for response efficacy and self-efficacy is adequate and indicates that ISA is an important precondition for the constructs. It is also necessary to consider the effect sizes (f^2) to discuss the strength of the direct effects on the paths between the latent constructs.

Table 4. Verdict on Structural Relationships of the Research Model

Hypotheses	Path coefficient	T-values	f^2	f^2 Effect
(H1): Perceived Vulnerability → Intention for CSB	0.09	1.23	0.01	No effect
(H2): Perceived Severity → Intention for CSB	0.20***	2.62	0.05	Weak
(H3): Response Efficacy → Intention for CSB	0.31***	4.02	0.11	Weak
(H4): Self-Efficacy → Intention for CSB	0.28***	3.67	0.09	Weak
(H5): ISA programs → Intention for CSB	0.15*	1.95	0.03	Weak
(H6): ISA programs → Perceived Vulnerability	-0.21***	2.89	0.05	Weak
(H7): ISA programs → Perceived Severity	0.16**	2.25	0.03	Weak
(H8): ISA programs → Response Efficacy	0.43***	6.02	0.23	Moderate
(H9): ISA programs → Self-Efficacy	0.50***	8.28	0.32	Moderate
(H10): Intention for CSB → Actual CSB	0.56***	8.29	0.45	Strong
(H11): Perceived Monitoring moderates INT-Actual CSB	0.18***	3.11	0.10	Weak

*p<0.10, **p<0.05, ***p<0.01
f^2 effect sizes: no effect (<0.02); weak (0.02-0.14), moderate (0.15-0.34); strong (above 0.34)

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

Next, bootstrapping with 5,000 subsamples was conducted to calculate t-statistics and further to evaluate the significance of the path coefficients (Hair et al. 2013). Table 2 illustrates path coefficients, t-values and f^2 effect sizes, which were used to quantify the size of an effect of an endogenous on an exogenous factor (Hair et al. 2013).

Finally, we conducted the mediation analysis. Contemporary mediation analysis suggests firstly focusing on the significance of the indirect variable (IV) for predicting the mediators, which is the case for all four PMT constructs. Secondly, the mediators should affect the dependent variable (DV), which is not the case for perceived vulnerability. Thirdly, the direct path between these variables (IV->DV) needs to be assessed. When removing the mediator, the path coefficient on this direct path should increase and be significant (Baron and Kenny 1986). The later condition holds for our remaining three mediation hypotheses (H5b: $p<.10$, H5c-d: $p<.01$). Finally, the Sobel test (Sobel 1982) confirmed these significant mediation effects after performing bootstrapping with replacement (H5b: $p<.10$, H5c-d: $p<.01$).

Discussion of the Results

Overall, our findings confirm the import roles of protection motivation and monitoring in establishing ISA programs that affect the employees' intentions for compliant security behavior. While we can also confirm that ISA programs have a positive weak direct effect on the intention for compliant security behavior, thereby supporting hypothesis H5, three constructs of protection motivation and especially coping appraisal act as a mediators allowing for indirect effects. We will discuss these results now in more detail.

In terms of coping appraisal, we detected moderate positive effects of ISA programs on response efficacy and self-efficacy, thereby supporting hypotheses H8 and H9. The results therefore confirm that coping appraisal is effectively improved by ISA programs. This can be explained by the common use of ISA programs to provide guidelines for employees on how to act and also information about the effectiveness of the actions to comply with the ISP (Bauer et al. 2013b). In addition, both coping appraisals are important variables in terms of mediating the effects of ISA programs on the intention to comply, thereby supporting hypotheses H5c and H5d. This means that improved response efficacy and self-efficacy are conditions which increase the positive effects of ISP programs on the intention for compliant security behavior. Subsequently, both constructs of coping appraisal have weak positive effects on the intention for a compliant security behavior, thereby supporting H3 and H4. This finding corresponds with (Ifinedo 2012; Meso et al. 2013) and contradicts prior research (Siponen et al. 2014b). Our results clearly indicate that employees, which belief that they can mitigate information security risks with their compliant behavior, have a higher intention to act according to the ISP.

With regard to threat appraisal, our results indicate that ISA programs have a weak positive effect on perceived severity, hence hypothesis H7 is supported. In fact, the ISA programs may utilize frightening fear-based communication as well as information to clarify the potential impacts, and therefore successfully highlight the possible negative impact of an information security threat (Kajzer et al. 2014). However, contrary to our expectations, ISA programs have negative effects on the other threat appraisals construct, perceived vulnerability, thereby contradicting hypothesis H6. We therefore assume that employees' consummation of an ISA programs help employees to deal with information security threats and risks, and, consequently, this leads to a decrease of the perceived probability of a security incident. This is also potentially dangerous and may lead to a false sense of security as employees may underestimate the possibility that their information system could be threatened (Albrechtsen and Hovden 2009). Further, perceived vulnerability has no direct effect on the intention for a compliant security behavior, thereby not supporting H1. Previous results showed positive effects (Ifinedo 2012; Siponen et al. 2014b). An explanation may refer to other environmental or contextual factors to explain this result (Hu et al. 2012; Padayachee 2012; Tsohou et al. 2013). Besides, perceived severity has a significant positive effect on intention, thereby supporting H2. While this result supports our theorization, it adds empirical evidence to mixed results reported in literature in terms of positive or negative effects of perceived severity on intention (Ifinedo 2012; Siponen et al. 2014b). It terms of mediating effects of ISA programs on the intention to comply, threat appraisals are not as important as coping appraisals. Only hypothesis H5b is weakly supported, while hypothesis H5a is rejected. It seems that ISA programs are more successful in terms of offering coping actions and relatively less effective it terms of actually increasing awareness about threats and risks. Employees may often miss connecting ISP content with the likelihood of a real danger (Bauer et al. 2013b). We need to recommend that future research should explore these relationships in more detail.

Finally, we confirm that perceived monitoring positively moderates the positive effects of intention to actual compliant security behavior, therefore supporting hypotheses H10 and H11. Our data analysis confirms a partial positive moderation effect of organizational monitoring on the intention-behavior link. However, we can assume that also other contextual factors influence this relationship (Hu et al. 2012; Padayachee 2012; Tsohou et al. 2013) and future research should address further contingencies.

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

The findings have also several implications for practice. First, ISA programs are currently well designed to increase employees' coping appraisal in terms of both, response efficacy and self-efficacy. This means that they are already effective in convincing employees about the value of the behavior and about how to behave, respectively. Second, in terms of threat appraisals, ISA programs seem to have adverse effects on perceived vulnerability based on our sample. In other words, ISA programs seem to lower the perception of the probability of an information security threat, maybe due to the fact that employees tend to protect themselves better after consuming ISA programs. We still recommend that ISA programs should communicate more the occurrence of real threats from media or inside the company and the concept of residual risks in order to increase the perceptions of vulnerability (Puhakainen and Siponen 2010). Nonetheless, the findings indicate that ISA programs eventually increase the intention for compliant security behavior. Third, ISA programs should communicate that employees are monitored, which strengthens the relationship between intention and actual compliant information security behavior.

Conclusion

Our study points to important theoretical implications with regard to PMT as prior literature has largely neglected to investigate the role of ISA programs and organizational monitoring to ultimately improve information security behavior. Our main findings illustrate that ISA programs affect employees' coping appraisals in terms of response and self-efficacy. Both variables are also mediators adding to the positive direct effects of ISA programs on the intention for compliant security behavior. Similarly, ISA programs have positive effects on employees' perceived severity, which positively affects the intention to comply with the ISP. However, ISA programs may have adverse effects on the perceived vulnerability possibly signaling a false sense of security. Especially these initial findings merit more attention in future research. Finally, perceived organizational monitoring is important as it partially positively moderates the well-established intention to actual behavior connection.

References

1. Albrechtsen E, Hovden J (2009) The information security digital divide between information security managers and users. Computers & Security 28:476-490
2. Baron RM, Kenny DA (1986) The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. Journal of Personality and Social Psychology 51:1173-1182
3. Bauer S, Bernroider EWN (2013) IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems. In: Janczewski L (ed) Proceedings of the International Conference on Information Resource Management 2013 (Conf-IRM 2013). Natal, p 1-4
4. Bauer S, Bernroider EWN (2013) IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from exploratory Case Study. In: Nunes MB (ed) Proceedings of the International Conference Information Systems 2013. IADIS Press Lissabon, p 30-38
5. 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. In: AIS SIGSEC Workshop on Information Security & Privacy (WISP2013). Milano
6. Behrend TS, Sharek DJ, Meade AW et al. (2011) The viability of crowdsourcing for survey research. Behavior Research Methods 43:800-813
7. D'arcy J, Hovav A (2008) Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics 89:59-71
8. Eminağaoğlu M, Uçar E, Eren Ş (2009) The positive outcomes of information security awareness training in companies – A case study. Information Security Technical Report 14:223-229
9. Floyd DL, Prentice-Dunn S, Rogers RW (2000) A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology 30:407-429
10. Goldstein J, Chernobai A, Benaroch M (2011) An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. Journal of the Association for Informaton Systems 12:606-631
11. Hagen JM, Albrechtsen E, Hovden J (2008) Implementation and effectiveness of organizational information security measures. Information Management & Computer Security 16:377-397
12. Hair JF, Hult GTM, Ringle CM et al. (2013) A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks: Sage

Bauer, Stefan, Bernroider, Edward. 2015. „The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," In *Lecture Notes in Computer Science (LNCS), Human Aspects of Information Security, Privacy, and Trust,* 154-164, Hrsg. Los Angeles.
The final publication is available at Springer via http://dx.doi.org/ 10.1007/978-3-319-20376-8_14

13. Hair JF, Sarstedt M, Ringle CM et al. (2011) An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science 40:414-433

14. Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47:154-165

15. Herath T, Rao HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18:106-125

16. Hu Q, Dinev T, Hart P et al. (2012) Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences 43:615-659

17. Ifinedo P (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31:83-95

18. Johnston AC, Warkentin M (2010) Fear Appeals and Information Security Behaviors: An Empirical Study. Mis Quarterly 34:549-566

19. Kajzer M, D'arcy J, Crowell CR et al. (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security 43:64-76

20. Lebek B, Uffen J, Neumann M et al. (2014) Information Security Awareness and Behavior: a theory-based literature review. Management Research Review 37:1049-1092

21. Meso P, Ding Y, Xu S (2013) Applying Protection Motivation Theory to Information Security Training for College Students. Journal of Information Privacy & Security 9:47-67

22. Milne S, Orbell PS, Orbell S (2000) Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory Journal of Applied Social Psychology 30:106-143

23. Orx (2014) ORX Report on Operational Risk Loss Data. In:Operational Riskdata eXchange Association

24. Padayachee K (2012) Taxonomy of compliant information security behavior. Computers & Security 31:673-680

25. Pahnila S, Siponen M, Mahmood MA (2007) Employees' Behavior towards IS Security Policy Compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE, Hawaii

26. Puhakainen P, Siponen M (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34:757-778

27. Ringle C, Wende S, Will A (2005) SmartPLS 2.0 (beta). In: Hamburg Uo (ed)

28. Rogers RW (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology 91:93-114

29. Sarstedt M, Ringle CM, Hair JF (2011) PLS-SEM: Indeed a Silver Bullet. The Journal of Marketing Theory and Practice 19:139-152

30. Siponen M, Mahmood MA, Pahnila S (2014) Employees' adherence to information security policies: An exploratory field study. Information & Management 51:217-224

31. Siponen M, Pahnila S, Mahmood MA (2010) Compliance with Information Security Policies An Empirical Investigation. IEEE Computer

32. Sobel ME (1982) Asymptotic confidence intervals for indirect effects in structural equation models. In: Leinhardt S (ed) Sociological Methodology. American Sociological Association, Washington DC, p 290-312

33. Tsohou A, Karyda M, Kokolakis S et al. (2013) Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems

34. Vance A, Siponen M, Pahnila S (2012) Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management 49:190-198

35. Workman M (2009) A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. Information and Organization 19:218-232

36. Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior 24:2799-2816

Bauer, Stefan, Chudzikowski, Katharina. 2015. „Mind the Threat! A Qualitative Case Study on Managing Information Security Awareness Programs in Central and Eastern European Banks," In *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Hrsg. Allen Lee, Puerto Rico.

Mind the Threat! A Qualitative Case Study on Information Security Awareness Programs in European Banks

Emergent Research Forum

Stefan Bauer
Vienna University of Economics and Business
Stefan.Bauer@wu.ac.at

Katharina Chudzikowski
University of Bath, School of Management
k.chudzikowski@bath.ac.uk

Abstract
This case study aims to analyze the dynamics in banks, which implement an information security awareness (ISA) program. In detail, we describe ISA programs in three major banks from three Central Eastern European countries. We examine how the specific context shapes different phases of its implementation. The contextual differentiation helps us to discover how specific characteristics of ISA programs affect employees' information security awareness, which is reflected by employees' perception of information security risks and threats. Moreover, the research contributes to state of the art behavioral information security research by discovering conflicts concerning compliant information security behavior from specific organizational perspectives. Stakeholders identify several conflicts, which affect compliant information security behavior. We use an embedded single-case study to investigate three implementation processes and how they are constructed in three banks in Central and Eastern Europe. We triangulate interview data and documents in the respective organizational context.

Keywords
Information security awareness program, information security compliance, tension between stakeholders.

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

Abstract
In organizations, users' compliance with information security policies (ISP) is crucial for minimizing information security incidents. To improve users' compliance, IS managers have implemented information security 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.

Keywords: Information Security Awareness, Design Recommendations for Information Security Awareness Programs, Users' ISP Compliance, Information Security Awareness Programs, User Perceptions.

Introduction

Financial institutions are increasingly threatened by data- and function-related information security (IS) risks and incidents (Goldstein et al., 2011; PricewaterhouseCoopers, 2014). Particularly for banks, confidentiality, integrity, and availability of information are absolutely required to guarantee the necessary levels of service quality, and hence to survive in the competitive market (Goldstein et al., 2011). The ongoing IS breaches in banks further demonstrate the importance of IS (ORX, 2014). 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 & 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). Hence, they are interested in minimizing their IS incidents to reduce their obliged capital reserves. Further, IS incidents cause reputational damage as well (Gillet et al., 2010). For all of these reasons, banks emphasize the prevention of IS incidents (Bauer & Bernroider, 2013).

Besides technology, human behavior is 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 & 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 & Willison, 2009). During the last decade, banks started to implement preventive controls such as IS policies (ISP), which introduce a binding standard concerning IS behaviors among all users, to avoid IS related loss incidents (Höne & Eloff, 2002).

IS policies outline specific security requirements, but they do not work alone (Warkentin & 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). Further, they have introduced structured ISA programs to educate the employees about IS risks and how to behave to comply with the ISP (Johnson, 2006). Accordingly, 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. These interventions build on the assumption that ISA leads to improved IS behavior and ISP compliance (Bulgurcu et al., 2010; Eminağaoğlu et al., 2009). For example, this should result in an increased protection of confidential information (Thomson & 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 article aims (i) first to address the challenge of IS management in banks to design effective ISA programs, and (ii) second to identify their perception and effects from the perspective of users. To support the first aim, we initially conducted a literature review highlighting current design practices of ISA programs. We then empirically evaluated whether these design practices are used in three case banks to enhance ISP compliance within the respective bank. Second, the study moved on to analyze how these ISA programs are perceived and which implications for users’ compliant IS behaviors may be determined. For this purpose, we analyzed responses from 10 interviews with IS managers and 23 interviews with users of the three banks to support the first and second aims, respectively. The interpretive approach resulted in the exploration of individual perceptions of users centering on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors. Finally, we consolidated the results by raising propositions regarding the relationship of ISA program designs and factors which are likely to influence users’ ISP compliance.

The remainder of the paper is structured as follows. First, we discuss the theoretical background of IS managers’ efforts, namely ISA programs, and factors which influence ISA programs. Then, we go on to describe the research methodology and process of empirical fieldwork. In chapter four, the main results of the study are presented. 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.

Literature Review

ISA Programs and Their Designs

Over the last two decades, ISA programs have received increasing attention because academics as well as practitioners have agreed on the necessity to shed light on this organizational intervention to enhance users' ISA (Silic & Back, 2014). Initially, ISA programs were found to be deterrent countermeasures (Straub & Welke, 1998), which require a systematic planning approach (Puhakainen & Siponen, 2010; Siponen, 2000). Previous research often describe similar concepts such as plan, do, check, act (PDCA) cycle models to visualize the continuous need of ISA building. Users' achieved ISA is a temporal state of mind, which has to be renewed periodically (Warkentin et al., 2012; Wilson & 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).

Until now, no common agreement has been made on the effective design of ISA programs (Karjalainen et al., 2013). Current literature offers several ISA program design recommendations and mixed results about the effectiveness of ISA programs (Albrechtsen, 2007; Eminağaoğlu et al., 2009). Effectiveness refers to the ability of the ISA programs to increase individuals' ISA and further improve users' ISP compliance. However, we assume that the contrary findings concerning ISA programs are likely due to the diversity of the design of the implemented ISA program in banks (Bauer et al., 2013; Shaw et al., 2009). Hence, we discuss significant communicational and structural design patterns to shed light on possible designs and approaches of ISA programs (see Figure 1).

The first group of ISA program design recommendations refers to communication aspects. Often, ISA interventions fail to affect users because they use a language that is too technocratic (Clarke et al., 2012). Further, recent studies found that specific personality types are more or less receptive to a specific kind of message or communication channel (Kajzer et al., 2014). More precisely, the initially proposed classic 'one to many' mass communication and the deterrent nature of ISA programs should change to more differentiated approaches, in which communication should match personality types (Kajzer et al., 2014). Moreover, users' emotional involvement can be achieved through several techniques by enforcing a two-way communication about IS (Albrechtsen & Hovden, 2010; Clarke et al., 2012; Spears & Barki, 2010). Reflection, either as collective or individual reflection of IS risks, is reported to have a high impact on users' ISP compliance (Albrechtsen & Hovden, 2010). However, another option is the use of role models communicated via role plays, which increase users' identification with the character in ISA programs; this identification results in more emotional involvement (Karjalainen et al., 2013). Similarly, feedback interventions can be used to emotionally involve users and can lead to a two-way communication about IS (Eminağaoğlu et al., 2009). Overall, several ways can be employed to tackle users' ISA through communication aspects to finally improve users' compliant IS behavior.

The structure of ISA programs is the next group of design recommendations under consideration. ISA programs should be strategically managed by considering the full PDCA cycle model (Wilson & Hash, 2003). Such PDCA cycle models are also recommended by conceptual academic literature about ISA programs (Siponen, 2000). 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 (Shaw et al., 2009). Last, but not least, a template of an ISA program does not fit in all entities of an organization, because there are cultural differences between countries and regions (Karjalainen et al., 2013).

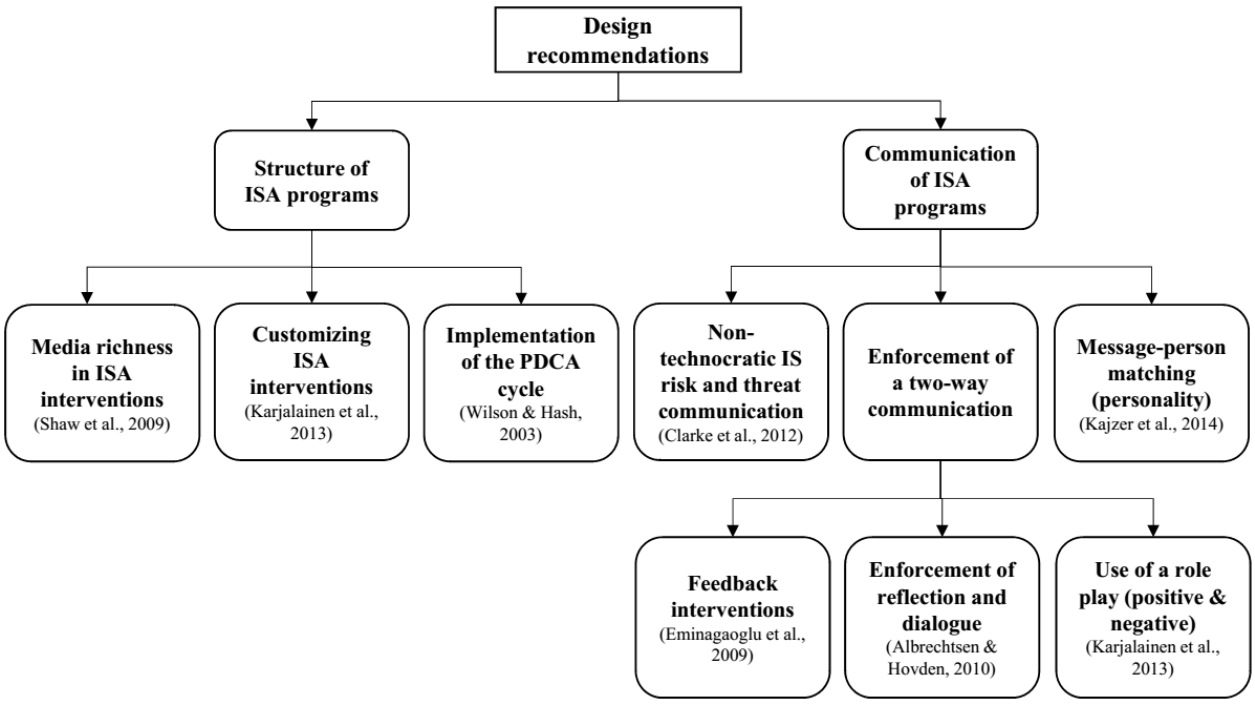


Figure 1 Design recommendations of ISA programs according to academic literature

Users' Compliance with ISP

Users regularly neglect to act according to their organizational ISP (Siponen, 2000), and current research offers a range of different explanations (Albrechtsen, 2007; Albrechtsen & Hovden, 2009; Posey et al., 2014). The perception of IS risks plays a significant role for acting compliant with banks' ISP (Albrechtsen, 2007). According to Posey et al. (2014), in the view of IS managers, unintentional ISP non-compliance of users is the greatest cause for security incidents. In contrast, users think that hackers and internet threats are the biggest IS risks, but they do not perceive themselves as a threat (Posey et al., 2014). However, previous research highlights that users struggle to estimate and recognize actual IS risks (Albrechtsen & Hovden, 2009; Posey et al., 2014).

Moreover, users' knowledge of the existence of the ISP and its content is an important pre-condition for ISP compliance (Wright, 2008). Previous research found that users' levels of ISP knowledge affect users' intentions to comply with ISP (Pahnila et al., 2013). Unintentional violations of the ISP might result from ignorance that ISP already exists or users not knowing the content of the ISP. Third, users and IS managers have different responsibilities concerning IS. For users, who have to perform in their job mainly as a marketing assistant or bank counter employee, information security is only a necessary side issue for them. In contrast, IS managers' primary role in their job is to ensure information security in the organization (Albrechtsen & Hovden, 2009, 2010).

Previous research highlights that employees should recognize the importance of information security (Lebek et al., 2014). Empirical work reported that from the viewpoint of IS managers, users do not take IS seriously and do not perceive the importance of IS for the organization (Albrechtsen & Hovden, 2009). Asked directly, however, users seem to perceive information security as important (Albrechtsen, 2007). This contrasting finding points at diverging perceptions from different user groups within an organization, which will be explored in this study.

Research Methods

Research Approach

In this study we use a multiple case study design (Cavaye, 1996; Yin, 2014), as each bank acts as a distinct bounded case. We are particularly interested in a contrasting case study design (Stake, 2005) as it illuminates the distinct design approaches of ISA programs as well as diverse factors influencing ISP compliance in each organizational setting. Furthermore, each organization is considered as an embedded case because it involves more than one unit of analysis (i.e. it relates to more than one branch and more than one individual user). In detail, one research case consists of interviews of branch as well as headquarter users, IS managers, and ISA program materials (e.g. intranet messages). 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. Specifically, we use inductive reasoning

to develop propositions and to contribute to the theoretical understanding of the ISP compliance and design recommendations for ISA programs (Eisenhardt, 1989). Figure 2 illustrates the research progress and stages.

Data Collection and Analysis

As part of the case study design, this study employs a qualitative research design including semi-structured interviews and the analysis of ISA program materials such as intranet messages or leaflets. For this purpose, we conducted interviews with two groups of employees over two stages: in particular, 23 interviews with users, and 10 interviews with IS managers (see for detail in Table A1 in the appendix). All interviews have been conducted in English, except the interviews in Gamma bank, which have been carried out in the German language. Following our sampling strategy, we initially identified 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.

For data collection, the stages in Figure 2 were deployed. As a part of the wider project, a focus group workshop was conducted as well to obtain a deeper understanding of IS and ISP compliance in 2013, in which potential research stakeholders were invited. After the workshop, we set up a semi-structured questionnaire targeting the responsible persons for ISA programs of our three case banks. Afterward, we started the first stage of qualitative fieldwork by interviewing from March to April 2013. After these deep insights in the design and implementation of ISA programs were provided by IS managers, we introduced the second and final stage by conducting qualitative interviews with users of the three case banks from September 2013 to June 2014.

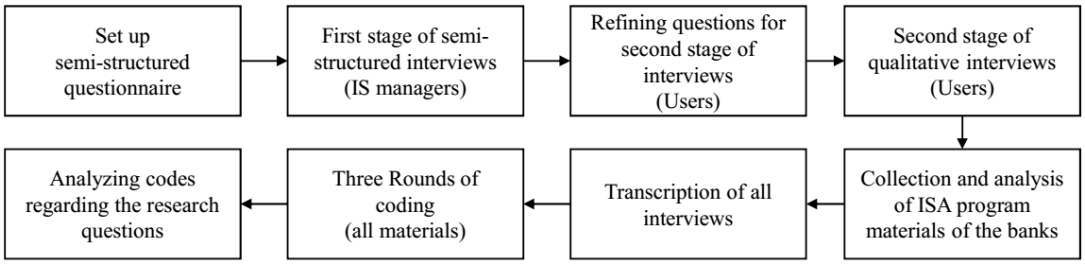


Figure 2 Research process

As a result of our sampling strategy, interviewees were included according to their different roles they hold in the organization (Myers & Newman, 2007). Table A1 indicates the position of the users, the interview types, and the stakeholder category. All interviews and organizations were anonymized to grant confidentiality (Sarker et al., 2013).

All interviews were transcribed and themes were coded inductively, developing first- and second-order categories using content analysis (Huberman & Miles, 1994; Mayring, 2003), which was supported with NVivo. In the first round, the research team inductively coded the interview data separately to generate specific conceptual categories and to meet quality criteria. After coding the interviews separately, the researchers met and communicated and mutually validated the codes. Based upon Mayring’s method, the coders first defined relevant text passages in their materials as units of analysis, paraphrased them, and then generalized them at a higher level of abstraction. Originally stemming from a grounded theory method, this procedure purposefully engages an inductive approach to show a reasonably sophisticated picture of themes in each organization.

Results

Building on the following case descriptions, we discuss our main results in the subsections below. First, we start with a case overview 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.

Case Overview

The three banks operate in Central Eastern Europe and are universal banks, which means that they are conducting the entire bandwidth of bank businesses. Since Basel II was enacted, they set up units for operational risk to manage risks related to humans, processes, and information systems. Additionally, the banks have IS departments responsible for ISA programs. Table 1 summarizes several facts about the banks and their ISA programs.

	Alpha bank	Beta bank	Gamma bank
Branches/users	150/3,000	650/11,000	500/6,000
Special facts about the bank	Eastern European bank with a long tradition	Conservative, rules-oriented CEE bank	Regional Central European bank

Table 1. Facts about the research cases

All three banks have some practices and established processes regarding IS in common. For example, if an employee is hired at a bank, he or she has to undergo a one-day training, including compliance training, in which IS is an important part. After this training, the users should have a basic level of knowledge about their respective ISP. Before users are allowed to begin with their work, they have to sign an acknowledgment of the ISP. However, all banks have developed their own data classification by which they categorize their data based on its level of sensitivity and the impact to the bank. Additionally, each bank has established an annual E-learning strategy, in which IS is addressed. IS managers are not satisfied with the implemented E-learning courses and mentioned that most users do not take it seriously, 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.

Alpha Bank - Interaction Approach

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

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 biweekly 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.

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 address 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.

Consideration of ISA Program Designs

The three banks have inconsistently implemented the design recommendations shown in Table 2 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.

	Alpha bank	**Beta bank**	**Gamma bank**
Structural design recommendations			
Media richness of ISA interventions (Shaw et al., 2009)	yes	yes	yes
Implementation of the full PDCA cycle (Wilson & Hash, 2003)	yes	yes	no
Customizing ISA interventions (Karjalainen et al., 2013)	no	no	no
Communicational design recommendations			
Non-technocratic IS risk and threat communication (Clarke et al., 2012)	yes	no	no
Message – person matching in regard to users' personalities (Kajzer et al., 2014)	no	no	no
Enforcement of a two-way communication			
Enforcement of reflection and dialogue (Albrechtsen & Hovden, 2010)	yes	no	no
Use of role models and role play (Karjalainen et al., 2013)	yes	no	no
Feedback interventions (Eminağaoğlu et al., 2009)	yes	no	no
Overall coverage level of design recommendations	**high**	**medium**	**low**

Table 2. Design recommendations of 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. 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. Unfortunately, the message-to-person matching with regard to users' personalities has not been considered in the researched ISA programs until now.

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. 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.

Employee Groups and Problematic IS Behaviors

Figure 3 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.

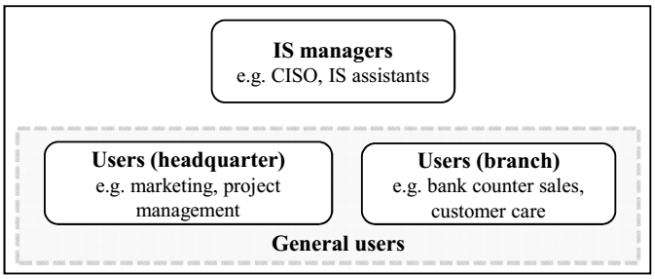


Figure 3 Overview of considered employee groups

The analysis revealed that the unintentional and intentional behavior of users is 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 policy, 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.

Factors Influencing ISP Compliance

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 information security 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.

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 responsibilities among a few users might be that the importance of IS in banks is not perceived 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.

Use of Neutralization Techniques by Users

Due to respondents' social desirability behavior, users were only asked if coworkers neutralize their ISP violations. 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.

Discussion

ISA programs in banks can be seen as complex and difficult controls which need to be designed and operationalized carefully to gain the desired improvements in compliant IS behaviors of employees. We analyzed three different banks which applied different types of ISA programs, including different coverage levels of design recommendations from literature, and identified responses to capture technical and behavioral implications from users, which again differ across banks and user groups. The following discussion builds up to a set of research propositions.

In terms of design recommendations, Alpha bank's ISA program design considered mostly all suggested design recommendations ("high coverage level of design recommendations"). Alpha bank has applied media richness (Shaw et al., 2009), an implementation of the full PDCA cycle (Wilson & 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 & Hovden, 2010). This design comprehensive strategy seems to be more effective than both of the less comprehensive strategies seen in the other two banks based on responses gained from users and IS managers. Implications include more positive situations in terms of the level of perceived IS risks, acknowledged responsibilities, the importance attached to IS and knowledge regarding the ISP, as well as the reduced mentioning of neutralization techniques observed among colleagues. This observation leads us to our first proposition:

Proposition 1. The incorporation of a comprehensive mix of design recommendations in ISA programs coupled with their controlled consumption by users is likely to lead to improved levels of behavioral ISP compliance.

More specifically regarding the structure of ISA programs, the PDCA cycle model was implemented by both the Alpha and Beta banks. Without an evaluation mechanism, the ISA programs are conducted largely without understanding the usefulness of the interventions. For example, some Gamma bank users mentioned that the ISA interventions are a form of self-congratulation of the security department. Therefore, without measuring the usefulness, an intervention may fail to address the context and user needs. Hence, our findings support the views about the importance of feedback mechanisms (Eminağaoğlu et al., 2009) and the usefulness of cycle models for managing ISA programs (Siponen, 2000; Straub & Welke, 1998; Wilson & Hash, 2003). Further, the respondents illustrated that IS managers often lacked a clear strategy for the mitigation of IS incidents and for their ISA program. The strategies driving the ISA programs of Beta and Gamma bank were less planned and more emergent in comparison with Alpha bank. The directions depended on current topics on a quarterly basis and on the yearly approval of resources. As a consequence, the single ISA interventions were not as well coordinated as a comprehensive strategy. Thus, the importance of a long-term planned strategy for managing an ISA program was barely covered by previous literature and extends previous findings.

Proposition 2. The implementation of a planned strategy for managing an ISA program is likely to lead to improved levels of behavioral ISP compliance.

The analyzed communicational aspects of ISA programs uncovered the implications of Alpha bank's best practices concerning their involvement of users. Alpha bank enforced involvement by feedback interventions in the form of quizzes and role plays. Users reported a high number of satisfaction and perceived usefulness in the follow up questionnaire. Hence, the underlying results support current studies regarding the enforcement of reflection and dialogue (Albrechtsen & Hovden, 2010), use of role models and role plays (Karjalainen et al., 2013), and feedback interventions (Eminağaoğlu et al., 2009), which all propose that a user involvement approach is beneficial for raising ISA. Furthermore, Alpha bank sets a positive example concerning non-technocratic IS risk communication. In the other banks, users reported that the ISP is not understandable and in particular reported that in Gamma bank's ISA program, the interventions were not well transported. Therefore, we provide empirical evidence adding to the study of Clarke et al. (2012), which states that non-technocratic IS risk communication is important. In contrast, Beta and Gamma bank did not implement any of the suggested design recommendations. Therefore, we raise another proposition in which we assume:

Proposition 3. The consideration of user involvement in an ISA program is likely to lead to improved levels of behavioral ISP compliance.

We also distinguished between different types of ISA programs, with Alpha Bank implementing an interaction approach, Beta Bank an incident approach, and Gamma bank an accountability approach. The interaction approach focuses on user involvement and helps the IS managers to get feedback about their ISA interventions and about employees' perception of actual IS risks. Beta bank's incident approach helps users to imagine actual IS risks, in contrast to Gamma bank's users, who report that they miss 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 the feeling of mistrust. Overall, every approach has some advantages.

Finally, the case banks neglected several design recommendations, which might have been useful for their ISA program. First, one possibility for improvement is an individualism mechanism (D'Arcy & Hovav, 2008), which enables the ISA intervention to fit the personality of the users (Kajzer et al., 2014). However, IS managers mentioned that such an individualism mechanism is difficult to establish in practice, because data about the personality of users is difficult to collect. Further, banks neglected to customize their ISA interventions (Karjalainen et al., 2013) to regional contexts, organizational entities, and specific IS risks according to employee groups. Some respondents mentioned that physical separation is a main challenge for IS as well as for the management of ISA programs, as users are distributed in several hundred branches among the countries. Additionally, ISA program managers reported that branch users take certain IS risks or they are threatened by specific IS risks only in certain regions.

Besides providing more empirical evidence for the existence of factors influencing ISP compliance, our research extends current qualitative state-of-the-art literature (Albrechtsen & Hovden, 2009; Posey et al., 2014) by calling for a more differentiated target audience concept. We showed that different groups of users in banks face different IS risks and have different needs of information in their work areas (e.g. headquarter vs. branch user). For example, branch users struggle more with safely logging on and off from the computers, 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.

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 finally to improved levels of behavioral ISP compliance.

While the level of knowledge of ISP is consistently low 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 importance in ensuring the organization's IS, because for them IS is guaranteed by IT personal, and hence their own responsibility is not perceived. This finding extends existing IS research by providing deep insights in the problematic branch-headquarter user distinction (Albrechtsen, 2007; Albrechtsen & Hovden, 2009; Kolkowska, 2011; Posey et al., 2014).

Intentional violations of banks' ISP are justified by users in the form of neutralization techniques, and hence we provide additional insights to existing research (Barlow et al., 2013; Siponen & Vance, 2010). Our study highlights that well-covered ISA programs diminish partially the use of neutralization techniques and enhance the likelihood that those users will follow the banks' ISP. Unfortunately, no case focused on communicating ISA interventions based on the prevention of neutralization techniques, such as Barlow et al. (2013) stated. Several users reported some well-known neutralization techniques, but astoundingly branch users are using more techniques such as 'appeal to higher loyalties' and 'defense of necessity' (Siponen & Vance, 2010). Branch as well as headquarter users utilize the technique 'denial of injury'. Our results add value to previous qualitative research on ISA (Albrechtsen, 2007; Albrechtsen & Hovden, 2009; Posey et al., 2014) by corroborating the theoretical and practical relevance of ISA programs for diminishing ISP non-compliance. According to the differentiation approach, we assume that ISA interventions, which more specifically target particular neutralization techniques of headquarter or branch users, could more effectively tackle neutralizing behaviors. Finally, we raise the following proposition in which we assume:

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

Implications for Practice

Banks should consider the suggested design recommendations to establish effective ISA programs. Structure as well as communication related design recommendations are useful, but it seems that a special emphasis on interactivity is most beneficial for increasing ISA. In particular, users' emotional involvement seems to be advantageous for the success of ISA programs; involvement can be achieved by a dialog with users (e.g. via role-plays or quizzes). Further, the lack of an evaluation mechanism causes a lack of strategic management, and ISA programs suffer from this deficiency. Hence, IS managers should introduce strategic planning in their repertoire by implementing PDCA cycle models with an evaluation mechanism.

Second, IS managers should overcome the ISP non-compliance through raising understanding for all employees. IS managers should evaluate the needs of single user groups regarding ISP compliance, and they might customize mass media interventions to make the groups of users more aware of IS risk. The structure of users in banks is common with other industries whose workforce consists of headquarter as well as branch users. The branch structure has some implications for ISA programs, such as the geographical distance. The design of ISA programs should overcome this issue in the future.

Third, three neutralization techniques have been identified as highly relevant in the 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. We assume that the use of neutralization techniques is interconnected with the user perceptions centering on IS risks, responsibilities, ISP importance, and knowledge. We assume if ISA programs are able to increase these factors, then the use of neutralization techniques might decrease.

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 be an important variable, and research could explore in more detail how involvement is reached through ISA interventions. Further, message-to-person congruence in ISA interventions was not analyzed through the underlying study because no case considered this factor. 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 the mixture of different types of ISA interventions is still needed.

Research on 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 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 a 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.

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 unique settings. Second, talking about security issues within the respective workplace could be biased by social desirability and other factors. 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.

Conclusion

The multiple case study revealed that different coverage levels of ISA program design recommendations is 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 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 particular in terms of headquarter and branch users.

References

Abawajy, J. (2012). "User preference of cyber security awareness delivery methods". *Behaviour & Information Technology*, Vo. 33, No. 3: pp. 237-248.

Albrechtsen, E. (2007). "A qualitative study of users' view on information security". *Computers & Security*, Vo. 26, No. 4: pp. 276-289.

Albrechtsen, E., & Hovden, J. (2009). "The information security digital divide between information security managers and users". *Computers & Security*, Vo. 28, No. 6: pp. 476-490.

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

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). "Don't make excuses! Discouraging neutralization to reduce IT policy violation". *Computers & Security*, Vo. 39, pp. 145-159.

Bauer, S., & Bernroider, E. W. N. (2013). "IT Operational Risk Management Practices in Austrian Banks: Preliminary Results from exploratory Case Study". *Proceedings of the International Conference Information Systems 2013*, Lissabon. pp. 30-38.

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2013). "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study". *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013)*, Milano.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness". *MIS Quarterly*, Vo. 34, No. 3: pp. 523-548.

Cavaye, A. L. M. (1996). "Case study research: a multi-faceted research approach for IS". *Information Systems Journal*, Vo. 6, No. 3: pp. 227-242.

Clarke, N., Stewart, G., & Lacey, D. (2012). "Death by a thousand facts". *Information Management & Computer Security*, Vo. 20, No. 1: pp. 29-38.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). "Future directions for behavioral information security research". *Computers & Security*, Vo. 32, pp. 90-101.

D'Arcy, J., & Hovav, A. (2008). "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures". *Journal of Business Ethics*, Vo. 89, No. S1: pp. 59-71.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research". *Academy of Management Review*, Vo. 14, No. 4: pp. 532-550.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). "The positive outcomes of information security awareness training in companies – A case study". *Information Security Technical Report*, Vo. 14, No. 4: pp. 223-229.

Gillet, R., Hübner, G., & Plunus, S. (2010). "Operational risk and reputation in the financial industry". *Journal of Banking & Finance*, Vo. 34, No. 1: pp. 224-235.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories". *Journal of the Association for Informaton Systems*, Vo. 12, No. 9: pp. 606-631.

Guo, K. H. (2013). "Security-related behavior in using information systems in the workplace: A review and synthesis". *Computers & Security*, Vo. 32, pp. 242-251.

Höne, K., & Eloff, J. H. P. (2002). "Information security policy—what do international information security standards say?". *Computers & Security*, Vo. 21, No. 5: pp. 402-409.

Hsu, C., Backhouse, J., & Silva, L. (2013). "Institutionalizing operational risk management: an empirical study". *Journal of Information Technology*, Vo. 29, No. 1: pp. 59-72.

Huberman, A. M., & Miles, M. B. (1994). "*Data management and analysis methods*". Thousand Oaks, CA: Sage Publications, Inc.

Jobst, A. A. (2007). "It's all in the data – consistent operational risk measurement and regulation". *Journal of Financial Regulation and Compliance*, Vo. 15, No. 4: pp. 423-449.

Johnson, E. C. (2006). "Security awareness: switch to a better programme". *Network Security*, Vo. 2006, No. 2: pp. 15-18.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). "An exploratory investigation of message-person congruence in information security awareness campaigns". *Computers & Security*, Vo. 43, pp. 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". *The Pacific Asia Conference on Information Systems (PACIS) 2013*.

Kolkowska, E. (2011). "Security Subcultures in an Organization - Exploring Value Conflicts". *The 19th European Conference on Information systems (ECIS) 2011*, Helsinki.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). "Information Security Awareness and Behavior: a theory-based literature review". *Management Research Review*, Vo. 37, No. 12: pp. 1049-1092.

Luthy, D., & Forcht, K. (2006). "Laws and regulations affecting information management and frameworks for assessing compliance". *Information Management & Computer Security*, Vo. 14, No. 2: pp. 155-166.

Mayring, P. (2003). "*Qualitative Inhaltsanalyse: Grundlagen und Techniken"* (8. ed.). Weinheim: Beltz.

Myers, M. D., & Newman, M. (2007). "The qualitative interview in IS research: Examining the craft". *Information and Organization*, Vo. 17, No. 1: pp. 2-26.

ORX, O. R. e. (2014). ORX Report on Operational Risk Loss Data. Retrieved from https://www.orx.org/Pages/ORXData.aspx [accessed on 12.12.2015]

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). "Information Security Behavior: Towards Multi-stage Models*"*. *Pacific Asia Conference on Information Systems (PACIS)*, Jeju Island (Korea).

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders". *Information & Management*, Vo. 51, No. 5: pp. 551-567.

PricewaterhouseCoopers. (2014). "Information Security Breaches Survey". *The Department for Business, Innovation and Skills, BIS/14/767*.

Puhakainen, P., & Siponen, M. (2010). "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study". *MIS Quarterly*, Vo. 34, No. 4: pp. 757-778.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). "Qualitative Studies in Information Systems: A Critical Review and Some Guiding Principles". *MIS Quarterly*, Vo. 37, No. 4: pp. iii-xviii.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). "The impact of information richness on information security awareness training effectiveness". *Computers & Education*, Vo. 52, No. 1: pp. 92-100.

Silic, M., & Back, A. (2014). "Information security: Critical review and future directions for research". *Information Management & Computer Security*, Vo. 22, No. 3: pp. 279 - 308.

Siponen, M. (2000). "A conceptual foundation for organizational information security awareness". *Information Management & Computer Security*, Vo. 8, No. 1: pp. 31-41.

Siponen, M., & Vance, A. (2010). "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations". *MIS Quarterly*, Vo. 34, No. 3: pp. 487-502.

Spears, J. L., & Barki, H. (2010). "User Participation in Information Systems Security Risk Management". *MIS Quarterly*, Vo. 34, No. 3: pp. 503-522.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). "Analysis of end user security behaviors". *Computers & Security*, Vo. 24, No. 2: pp. 124-133.

Straub, D. W., & Welke, R. J. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making". *MIS Quarterly*, Vo. 22, No. 4: pp. 441-469.

Thomson, M. E., & von Solms, R. (1998). "Information Security Awareness: Educating the Users effectively". *Information Management & Computer Security*, Vo. 6, No. 4: pp. 167-173.

Warkentin, M., Straub, D., & Malimage, K. (2012). "Featured Talk: Measuring Secure Behavior: A Research Commentary*"*. *Annual Symposium of Information Assurance & Secure Knowledge Management*, Albany, NY.

Warkentin, M., & Willison, R. (2009). "Behavioral and policy issues in information systems security: the insider threat". *European Journal of Information Systems*, Vo. 18, No. 2: pp. 101-105.

Wilson, M., & Hash, J. 2003. "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology (NIST) Special Publication 800-50, Gaithersburg.

Wright, C. S. (2008). "Assessing Security Awareness and Knowledge of Policy": Syngress *The IT Regulatory and Standards Compliance Handbook:: How to Survive Information Systems Audit and Assessments* pp. 161-194.

Yin, R. K. (2014). "*Case Study Research: Design and Methods"* (5 ed.). Thousand Oaks: Sage Publications, Inc.

Appendix

Table A1 Interview statistics

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 Controlling 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 A1: Interview statistics (all interviews face-to-face, average duration 33 minutes)

Table A2 Coding scheme

Codes: main-categories	Short description	Total instances
ISA program related codes		
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

Table A2. Coding scheme