COMPUTERS & SECURITY 68 (2017) 145–159

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

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

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

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

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

ARTICLE INFO

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

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

ABSTRACT

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

1. Introduction

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

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

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

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

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

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

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

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

2. Conceptual background

2.1. *ISA programs and their designs*

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