Winter 12-14-2013

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

Stefan Bauer
Vienna University of Economics and Business Administration, 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

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

Stefan Bauer[1]
Vienna University of Economics and Business

Edward W. N. Bernroider[2]
Vienna University of Economics and Business

Katharina Chudzikowski
University of Bath, School of Management

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 effectivenessof experimental and proactive ISA controlling. The outcome provides input for practice in the area of ISA building in the financial sector.

[1] Corresponding author: Stefan.Bauer@wu.ac.at.

[2] Corresponding author: Edward.Bernroider@wu.ac.at.

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

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 et al. 2013). 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 et al. 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 et al. 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.

THEORETICAL FOUNDATION AND RESEARCH

Taxonomy of End User Behavior

The underlying research considers employees as enablers of IT operational loss events. Desir-able 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 1.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 may 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 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.

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 et al. 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 2012), we categorize ISA delivery methods in conventional, instructor-led and online delivery methods. Table 2 indicates ISA delivery methods and their ad-vantages and disadvantages (Abawajy 2012).

Table 2.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 can be overlooked
	Employee newspaper	+ can convey a number of messages at the same time + tracking methods	- message can be overlooked - often seen as spam
Instructor-led delivery methods	Formal presentations and training	+ instructor is able to perceive non-verbal 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 it 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 sessions with minimal time or thought - become monotonous - fails to challenge user - 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 et al. 2006). Hence a continuous ISA building process is essential to increase employees' level of aware-ness (Puhakainen et al. 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 et al. 2005). In large organizations different subcultures exists (Kolkowska 2011). 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.

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 et al. 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 et al. 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.

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.

RESEARCH METHODOLOGY

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 et al. 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 et al. 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 et al. 2001). Hence, the epistemology of the research is interpretive paradigm.

Research context

The underlying research focuses on universal banks. Universal banks underlie several regulations in consideration of IT (Luthy et al. 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 rea-sons for design decisions such as cultural factors and their implications.

Data collection and analysis

We conducted first ten semi-structured qualitative interviews, which took place from July to September 2013 (see Table 3). 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 3 .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 de-fined 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 organizational unit.

PRELIMINARY RESULTS

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.

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.

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 4 provides an overview about the used delivery methods in the researched banks.

Table 4. 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).

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 et al. 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 stand-ard, 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 employ-ees really got the meaning of the article. By contrast, one of the researched banks has con-ducted 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 control-ling 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.

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.

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 Information 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. 2005."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. 2011."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. QualitativeInhaltsanalyse: Grundlagen undTechniken, (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 Conducting Mixed Methods Research in Information Systems," MIS Quarterly (37:1), pp 21-54.