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

Stefan Bauer(✉) and Edward W.N. Bernroider

Vienna University of Economics and Business, Vienna, 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

1 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 [23]. 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) [24]. Especially for banks, much is at risk, because an information security breach can lead to enormous reputational and operational damages [10].

To mitigate these risks, banks have implemented employee centric information security awareness (ISA) programs to actively protect their information assets [5]. An increased awareness concerning information security risks and threats is by many considered as the most cost-effective control of an organization [11]. ISA programs

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 154–164, 2015.
DOI: 10.1007/978-3-319-20376-8_14

make employees sensitive to foster security of organizations' information systems and be aware of information security risks [8]. Actual topics for ISA programs are, among others, phishing attacks, social engineering, passwords security, secure internet use and clear screen policy [5].

In general, Protection Motivation Theory (PMT) is used to discover motivational influences on the intention for a compliant security behavior [17, 28]. 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 [35]. 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.

2 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 [20]. The PMT addresses the determination of fear appeals and how individuals cope with the danger brought about by information security risks and threats [17, 28]. PMT has been considered as one the most powerful theories explaining individuals' intentions to engage in compliant actions [9, 20]. In the context of information security compliance, prior studies reported positive effects of all constructs of PMT on self-reported behavioral intentions [20, 21, 30, 36]. 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.

2.1 The Role of Protection Motivation Theory

PMT has been repeatedly examined and discussed in the extant behavioral information security literature [14, 15, 17, 21, 30, 34, 36]. The original theory builds upon threat and coping appraisal. Threat appraisal consists of the constructs perceived vulnerability and perceived severity of an event [30]. Perceived vulnerability is defined as an individual's

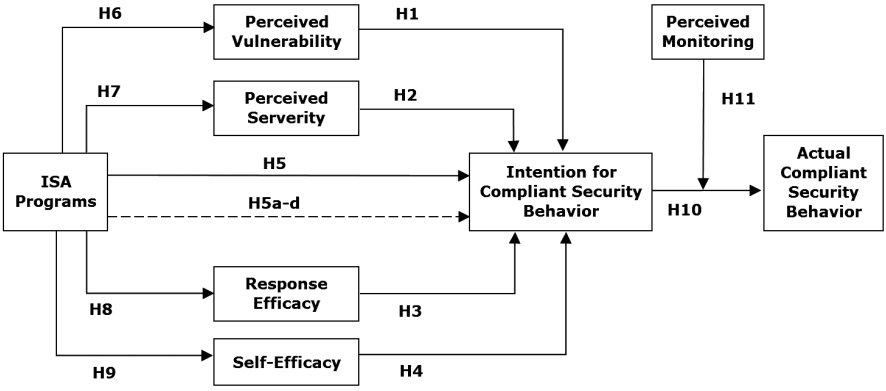

Fig. 1. Research model and hypotheses

perception of the probability of an information security incident, which in our context is caused by behavioral non-compliance with the ISP [17]. In contrast, perceived severity reflects the impact of an information security incident caused by non-compliance with the ISP [17, 31]. Previous research has shown mixed results concerning significant effects of perceived vulnerability and perceived severity on intention for compliant security behavior [15, 17, 25, 30]. Nonetheless, meta studies showed significant low positive effects [9, 20], 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 [9, 22]. Response efficacy is the expectancy of the employee that the threat or risk can be mitigated by conducting the ISP compliant security behavior [20], 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 [17, 25, 30]. In terms of, response efficacy previous research provides mixed results with no or marginally significant impacts [18, 25, 31] and positive impacts on compliant security behavior [17]. 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.

2.2 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 [5, 33].

In practice, ISA programs vary from bank to bank and different methods are used to make their employees more aware [4, 5]. ISA programs can be structured as intense and coordinated campaigns or simply consist of several isolated initiatives [5, 19]. An increased ISA through such programs can lead to improvements of employees' security compliance behavior [8]. Hence, we generally assume that ISA programs positively affect the intention for compliant security behavior [3]. 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).

ISA programs usually highlight current information systems risks and threats, such as those related to phishing or other social engineering attacks [5]. 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 [5]. 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.

2.3 The Role of Perceived Monitoring

Behavioral theories basing on self-reported data often examine the relationship between behavioral intent and actual behavior [20]. The correlation of these two constructs is assumed in the Theory of Planned Behavior as well as in PMT [20]. Hence, a variety of studies have already confirmed the significance of this relationship in behavioral information security context [25, 30, 31]. 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 [20]. Especially in the banking context, money is data in the information systems and banks need to monitor how employees are acting [5]. 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.

3 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 [7, 16, 17, 31]. 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 multi-stage 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 [6]. However, our sample seems to be biased towards younger male professionals. It consists of 135 men and 48 women, 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 [12] with SmartPLS [27]. We carefully considered all quality and validity criteria following current recommendations [12, 13, 29].

4 Validation of the Measurement Model

The measurement model was tested with all quality and validity criteria required by contemporary recommendations [12, 13, 29]. 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 [12]. Overall, all considered quality and validity criteria meet the contemporary recommendations.

Table 1. 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			

5 Evaluation of the Structural Model

We firstly conducted a PLS-SEM analysis to test the direct effects of PMT's latent constructs and examine the proposed hypotheses. As Fig. 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 [20, 30] and recommendations from scholarly research [12]. In contrast, R^2 values of perceived vulnerability and perceived severity are low. Furthermore, the achieved level of R^2 for response efficacy

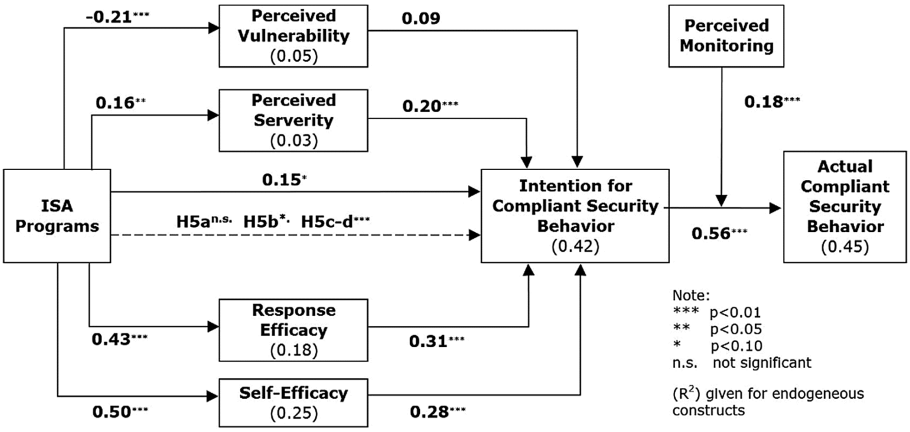

Fig. 2. Empirical results

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 2. 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)

Next, bootstrapping with 5,000 subsamples was conducted to calculate t-statistics and further to evaluate the significance of the path coefficients [12]. 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 [12].

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 [2]. The later condition holds for our remaining three mediation hypotheses (H5b: $p < .10$, H5c–d: $p < .01$). Finally, the Sobel test [32] confirmed these significant mediation effects after performing bootstrapping with replacement (H5b: $p < .10$, H5c–d: $p < .01$).

6 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 [5]. 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 [17, 21] and contradicts prior research [30]. 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 [19]. 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 [1]. Further, perceived vulnerability has no direct effect on the intention for a compliant security behavior, thereby not supporting H1. Previous results showed positive effects [17, 30]. An explanation may refer to other environmental or contextual factors to explain this result [16, 24, 33]. 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 [17, 30]. 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 [5]. 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 [16, 24, 33] and future research should address further contingencies.

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 [26]. 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.

7 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.: The information security digital divide between information security managers and users. Comput. Secur. **28**(6), 476–490 (2009)
2. Baron, R.M., Kenny, D.A.: The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. J. Pers. Soc. Psychol. **51**(6), 1173–1182 (1986)
3. Bauer, S., Bernroider, E.W.N.: 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, pp. 1–4 (2013)
4. Bauer, S., Bernroider, E.W.N.: IT operational risk management practices in austrian banks: preliminary results from exploratory case study. In: Nunes, M.B. (ed.) Proceedings of the International Conference Information Systems 2013, pp. 30–38. IADIS Press, Lissabon (2013)
5. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: 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 (WISP 2013), Milano (2013)
6. Behrend, T.S., Sharek, D.J., Meade, A.W., et al.: The viability of crowdsourcing for survey research. Behav. Res. Methods **43**(3), 800–813 (2011)
7. D'arcy, J., Hovav, A.: Does one size fit all? Examining the differential effects of is security countermeasures. J. Bus. Ethics **89**(1), 59–71 (2008)
8. Eminağaoğlu, M., Uçar, E., Eren, Ş.: The positive outcomes of information security awareness training in companies – a case study. Inf. Secur. Tech. Rep. **14**(4), 223–229 (2009)
9. Floyd, D.L., Prentice-Dunn, S., Rogers, R.W.: A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. **30**, 407–429 (2000)
10. Goldstein, J., Chernobai, A., Benaroch, M.: An event study analysis of the economic impact of it operational risk and its subcategories. J. Assoc. Inf. Syst. **12**, 606–631 (2011)
11. Hagen, J.M., Albrechtsen, E., Hovden, J.: Implementation and effectiveness of organizational information security measures. Inf. Manag. Comput. Secur. **16**, 377–397 (2008)
12. Hair, J.F., Hult, G.T.M., Ringle, C.M., et al.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage, Thousand Oaks (2013)
13. Hair, J.F., Sarstedt, M., Ringle, C.M., et al.: An assessment of the use of partial least squares structural equation modeling in marketing research. J. Acad. Mark. Sci. **40**, 414–433 (2011)
14. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. **47**, 154–165 (2009)

15. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**, 106–125 (2009)
16. Hu, Q., Dinev, T., Hart, P., et al.: Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. **43**, 615–659 (2012)
17. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. **31**, 83–95 (2012)
18. Johnston, A.C., Warkentin, M.: Fear appeals and information security behaviors: an empirical study. MIS Q. **34**, 549–566 (2010)
19. Kajzer, M., D'arcy, J., Crowell, C.R., et al.: An exploratory investigation of message-person congruence in information security awareness campaigns. Comput. Secur. **43**, 64–76 (2014)
20. Lebek, B., Uffen, J., Neumann, M., et al.: Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. **37**, 1049–1092 (2014)
21. Meso, P., Ding, Y., Xu, S.: Applying protection motivation theory to information security training for college students. J. Inf. Priv. Secur. **9**, 47–67 (2013)
22. Milne, S., Orbell, P.S., Orbell, S.: Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. J. Appl. Soc. Psychol. **30**, 106–143 (2000)
23. Orx: ORX report on operational risk loss data. In: Operational Riskdata eXchange Association (2014)
24. Padayachee, K.: Taxonomy of compliant information security behavior. Comput. Secur. **31**, 673–680 (2012)
25. Pahnila, S., Siponen, M., Mahmood, M.A.: Employees' behavior towards is security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS 2007). IEEE, Hawaii (2007)
26. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Q. **34**, 757–778 (2010)
27. Ringle, C., Wende, S., Will, A.: SmartPLS 2.0 (beta). In: Hamburg Uo (ed.) (2005)
28. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change. J. Psychol. **91**, 93–114 (1975)
29. Sarstedt, M., Ringle, C.M., Hair, J.F.: PLS-SEM: indeed a silver bullet. J. Mark. Theory Pract. **19**, 139–152 (2011)
30. Siponen, M., Mahmood, M.A., Pahnila, S.: Employees' adherence to information security policies: an exploratory field study. Inf. Manag. **51**, 217–224 (2014)
31. Siponen, M., Pahnila, S., Mahmood, M.A.: Compliance with information security policies an empirical investigation. IEEE Comput. **43**(2), 64–71 (2010)
32. Sobel, M.E.: Asymptotic confidence intervals for indirect effects in structural equation models. In: Leinhardt, S. (ed.) Sociological Methodology, pp. 290–312. American Sociological Association, Washington DC (1982)
33. Tsohou, A., Karyda, M., Kokolakis, S., et al.: Managing the introduction of information security awareness programmes in organisations. Eur. J. Inf. Syst. **24**(1), 38–58 (2013)
34. Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. **49**, 190–198 (2012)
35. Workman, M.: A field study of corporate employee monitoring: attitudes, absenteeism, and the moderating influences of procedural justice perceptions. Inf. Organ. **19**, 218–232 (2009)
36. Workman, M., Bommer, W.H., Straub, D.: Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. **24**, 2799–2816 (2008)