Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance

Ioanna Topa(✉) and Maria Karyda

University of the Aegean, Mytilene, Greece
{itopa, mka}@aegean.gr

Abstract. Organizations apply information security policies to foster secure use of information systems but very often employees fail to comply with them. Employees' security behavior has been the unit of analysis of research from different theoretical approaches, in an effort to identify the factors that influence security policy compliance. Through a systematic analysis of extant literature this paper identifies and categorizes critical factors that shape employee security behavior and proposes security management practices that can enhance security compliance. Research findings inform theory by identifying research gaps and support security management.

Keywords: Security behavior · Information security policy compliance

1 Introduction

Organizations implement security measures to secure their information infrastructure, business processes and services. In order to be resilient in a rapidly changing environment, enterprises invest not only on technical countermeasures, but also employ socio-organizational practices such as security policies to foster security behavior. An Information Security Policy (ISP) is generally "the statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" [5]. However, having an information security policy doesn't necessarily lead to user conformity. Employees often fail to comply with security policies while pursuing to perform their duties in the most effective and timely manner [9], as following ISPs may entail additional effort and time. Furthermore, in many cases employees are not aware of the importance of following ISPs and show little interest in complying [18].

Relative research has identified numerous factors that influence users to comply with ISPs or fail to do so; however, information security management lacks an overall view of what shapes security behavior so as to improve security compliance.

This paper provides an in-depth review of relevant research and a classification of factors that have been identified as influencing security behavior. The analysis provided can be used as a roadmap for security managers who want to create ISPs that gain the approval of users and also it can serve as the basis for implementing effective security management, by considering the impact of specific factors on users' security behavior and intention to comply with the information security policy [24].

S. Fischer-Hübner et al. (Eds.): TrustBus 2015, LNCS 9264, pp. 169–179, 2015.
DOI: 10.1007/978-3-319-22906-5_13

Section 2 analyzes relevant literature and identifies different factors that influence ISP compliance. Section 3 provides a classification of the factors identified so far, which inform security management and provide suggestions for improving compliance. Finally, research findings and indications for future research are presented.

2 Identifying Factors that Influence Security Behavior

Several relevant studies focus on the individual to identify factors that motivate security behavior in association with users' intentions and attitudes. Lebek et al. [20] through a literature review, found that the constructs of Theory of Reasoned Action (TRA)/ Theory of Planned Behavior (TPB) *(attitude, subjective norms and perceived behavioral control, which consists of self efficacy and controllability*), are good predictors of the intention to comply with the ISP. They also found that *organizational commitment*, *perceived effectiveness* of the employee's actions and *technology awareness* can also influence users' intention to comply. Authors argue that actual behavior can't be accurately assessed, for reasons such as that intentions do not necessarily lead to expected behavior [20] and that new methods need to be developed in order to measure actual behavior [21]. In the same direction, Zhang et al. [4] show that *perceived behavioral control* and *attitude* have a significant impact on intention towards complying with ISPs. *Perceived security protection mechanisms* (a term similar to *response efficacy*) were found to have a negative impact on the intention towards complying [4]; this implies that if employees estimate that there is strong technical protection to secure organizational assets, their intention to comply might weaken.

Sommestad et al. [11] focus on the individual to identify that *beliefs* (perceived behavioral control, threat appraisal, descriptive norm, response efficacy) and *values* (perceived value congruence, perceived legitimacy, information security awareness), play a critical role for user compliance with security policies. They also suggest that *rewards and punishments* are poor predictors of compliance. Son [25] found that *perceived value congruence* and *perceived legitimacy* influence the behavior of employees significantly and yield better results compared to factors based on extrinsic motivation such as perceived deterrent severity and perceived deterrent certainty.

Ifinedo [24] draws on Protection Motivation Theory and the Theory of Planned Behavior to show that *perceived vulnerability, response efficacy, self-efficacy, attitude towards compliance with the ISPs* and *subjective norms* influence the intention to comply with the ISPs. This study illustrates how employees are influenced by their colleagues, by their superiors and by other people in the organization's environment in terms of security compliance.

Siponen et al. [16], drawing also on Protection Motivation Theory, show that *visibility* (meaning the degree to which individuals have access to security related material both inside and outside the organization), and *normative beliefs* influence *threat appraisal*, which has an impact on the intention of an individual to comply with ISPs. Siponen et al. [15] study the two constructs of threat appraisal separately and show that *perceived vulnerability* and *perceived severity* have a significant effect on intention. Their study also identifies that *self-efficacy, attitude and normative beliefs* influence the intention towards complying that strongly predicts actual compliance.

Pahnilla et al. [13] also identified the role of *threat appraisal* and *coping appraisal* in user attitude. They found that *information quality (*meaning how useful, clearly stated and informative an ISP is), has a significant effect on actual compliance, and that *normative beliefs*, *attitude* and *habits* influence users' intention to comply. An interesting point following from this research is that security managers should encourage employees to comply with the ISPs, through habit. This study also suggests that *sanctions* have an insignificant impact on employee's intention to comply with the ISPs. Pahnilla et al. [12] also studied the impact of threat and coping appraisal on the employees' intention to comply and found that employees' intention who have high knowledge of the ISPs was influenced by *perceived vulnerability, perceived severity, response efficacy,* whereas employees' intention with low knowledge of the ISPs was only influenced by *perceived severity and response efficacy*. In both cases intention had high impact on actual compliance.

Herath and Rao [9], combining Protection Motivation Theory with Deterrence Theory and the Decomposed Theory of Planned Behaviour, found that *perceived severity* has a significant effect on user attitude and that social influence (*subjective and descriptive norms*) are good predictors of the intention to comply. Furthermore, this study shows that when employees believe that complying with a security policy entails costs such as time, effort, etc., they are likely to form negative feelings towards security policies. Therefore, *response costs* have a negative influence on the attitude to compliance. On the other hand, when employees feel that their compliance will benefit the organization, they may develop positive feelings towards this behavior and adopt it. As a result, employees' *response efficacy (effectiveness of a person's action)* has a significant impact on the attitude towards compliance. The same thing applies to *self-efficacy*, which influences attitude and intention towards complying with security policies. Another interesting finding is that *resource availability* has a significant effect on self-efficacy, which in turn influences intention. This indicates that security trained employees who have direct access to security policies, feel that they have the ability to comply with the ISPs and are more likely to comply with them. Furthermore *organizational commitment* has significant impact on intention to comply. Finally, according to this study *detection certainty* has a significant impact on the intention to comply, whereas the severity of punishment influences employees' intention in a negative way. In a following study, Herath and Rao [10] confirm that employees are more likely to conform to ISPs if they know that they will be caught, whereas the more severe the punishment is, the less willing they are to comply. They also show [10] that both *social influence* and *perceived effectiveness* (describing it similarly to response efficacy) have an impact on the intention to comply.

The role of automatic behaviors, such as habits, is further studied by Vance et al. [17] who show that habits influence *perceived vulnerability*, *perceived severity*, *response efficacy* and *self-efficacy* and that perceived vulnerability, rewards, response-efficacy and response cost have a negative impact on users' intention to comply with the ISPs. They also identify that *perceived severity* and *self-efficacy* have a significant effect on the intention to comply.

Bulgurcu et al. [5] studied the impact of the antecedents of attitude on intention to comply with the ISPs using the principles of Rational Choice theory [1]. Their study is based on the idea that individuals predict the possible outcomes of an event and depending on the perceived cost or benefit of the outcome they either adopt or refrain

from a specific action [5]. They also found that *attitude*, *normative beliefs* and *self-efficacy to comply* have a significant impact on the intention to comply with the ISPs. Finally, they identified that *Information Security Awareness* influences employees' attitude towards compliance with the ISPs.

Other studies approach security behavior through the lens of technology oriented theories such as the Technology Acceptance Model (TAM) [7]. Dinev and Hu [8] explored the factors that influence users' intention towards the use of protective technologies and found that *technology awareness has* a significant impact on the intention to use a protective technology.

One study conducted by D'Arcy et al. [6] shows that if users are aware of the ISPs of their organization, the existing SETA programs and the computer mechanisms that are in place, they are less likely to engage in misuse of the ISPs. Similarly, in the case of ISP compliance, Al-Omari et al. [2] employ TAM to show that user awareness of information security policies, information security, security awareness and training programs, computer monitoring, along with self-efficacy and controllability have a significant effect on the *perceived usefulness* of *protection* and *perceived ease of use*, which in turn guide users' intention to comply with security policies.

Summarizing, relevant literature has identified several factors that influence users' security behavior. However, different terms are often used to describe similar concepts, while different theoretical approaches show emphasis on different factors, making it extremely hard for security management to navigate through relative research and take advantage of important findings. Though taxonomies have been proposed, e.g. Padayachee's [22] classification of security compliant behavior, security management needs a higher level framework that can enhance security policy implementation. Table 1 summarizes our analysis of relevant literature.

3 Enhancing Security Policy Compliance

Literature analysis shows that a wide variety of factors influence users' security behavior and ISP compliance. Depending on the theoretical background followed, different studies stress the importance of specific factors, while ignoring others. Security management needs the complete picture in order to develop a security-oriented culture, where security practices become part of the organizational routine [19].

Different factors that have been identified can be grouped into three courses of action that security management needs to pursue in order to foster security policy compliance and influence users' security behavior: (i) address individual issues that hinder compliance (e.g. habits), (ii) create a suitable organization setting (e.g. rewards and sanctions) and (iii) take into consideration technology aspects (e.g. usability of security controls), as shown in Fig. 1.

3.1 Addressing Individual Factors

Individual beliefs and perceptions play a critical role in security behavior. Thus, security managers need to provide users with information with regard to information

Table 1. Critical factors that influence security behavior

Factors	Description	Relevant studies
Threat appraisal (or Security breach Concern level)	Users' evaluation of possible threats and their severity.	[9, 13, 16]
Perceived Severity (or Perceived Severity of Security Breach)	Users' perceptions on the severity of the impact of security threats.	[9, 12, 15, 17]
Perceived Vulnerability (or Perceived Probability of Security Breach)	Users' estimation on how possible the occurrence of a security threat is.	[12, 15, 17, 24]
Self-efficacy	Users' evaluation of how capable they are in following ISPs.	[2, 5, 9, 15, 16, 17, 24]
Response efficacy (or Perceived Effectiveness or Perceived Security Protection mechanisms)	Users' perception of the effectiveness of security controls and ISP compliance.	[4, 9, 10, 12, 16, 17, 24]
Response cost (or Cost of compliance)	User's perception of the possible negative consequences, such as inconvenience, additional effort and time, that derive from ISP compliance.	[5, 9, 17]
Perceived Behavioral Control, (Self efficacy and Controllability)	Users' estimation on how easy compliance is and how much control they have on carrying out security tasks.	[4, 8]
Information Security Awareness	Knowledge of information security and of the specific ISP of the organization.	[5]
General Information Security Awareness	Knowledge of information security.	[2, 5, 6]
ISP Awareness	Knowledge of the content of specific ISPs.	[2, 6]
Awareness of SETA programs	Knowledge of Security Awareness and Training Programs.	[2, 6]
Awareness of monitoring mechanisms	Knowledge of the monitoring mechanisms in place.	[2, 6]
Technology Awareness	Knowledge and consciousness of a technological issue that leads the individual to search for possible solutions.	[8]
Habits	Actions conducted unconsciously.	[13, 18]
Perceived Ease of Use	Users' belief of how easy a particular technology is.	[2]
Perceived Usefulness	Users' belief of whether a particular technology will be more efficient.	[2, 8]

(*Continued*)

Table 1. (*Continued*)

Factors	Description	Relevant studies
Rewards	Possible rewards include pay raises, personal mention, promotions, etc.	[5, 18]
Sanctions	Penalties, such as fines, following non compliance.	[5]
Punishment Severity (or Perceived Punishment Severity)	Users' perceptions on the level of punishment for non compliance.	[9, 10]
Punishment Certainty (or Perceived Punishment Certainty)	Users' estimation of the possibility to be detected for non compliance.	[9, 10]
Perceived Cost of Noncompliance	Sanctions, negative feelings and vulnerability of resources connected to failure to comply with the ISPs.	[5]
Perceived Benefit of Compliance	Positive feelings, rewards and decreased vulnerability in resources that result from compliance with the ISPs.	[5]
Perceived Legitimacy	The extent to which users consider the ISPs as appropriate, desirable and just.	[25]
Perceived Value Congruence	The extent to which users share the same values with employers.	[25]
Information Quality	Users' perceived quality and usefulness of the information included in the ISPs.	[12, 13]
Facilitating conditions (or Resource Availability or Controllability or Visibility)	Resources provided to facilitate compliance, including encouragement, time, help from experts, access to ISPs, etc.	[2, 8, 9, 13, 16]
Organizational commitment	The degree to which users share organizational goals.	[9]
Subjective norms (or Normative beliefs)	Perceived expectations of colleagues and superiors.	[2, 5, 9, 10, 13, 15, 16, 24]
Descriptive norms (or Peer behavior)	Users' belief that they should follow their colleagues' behavior.	[9, 10]

security threats and their severity [9, 12, 15, 17], through seminars, email notifications and other security awareness practices. However, as literature suggests, communicating security information, needs to be combined with security training so as to enhance user's confidence on their ability to use security controls and comply with the ISPs

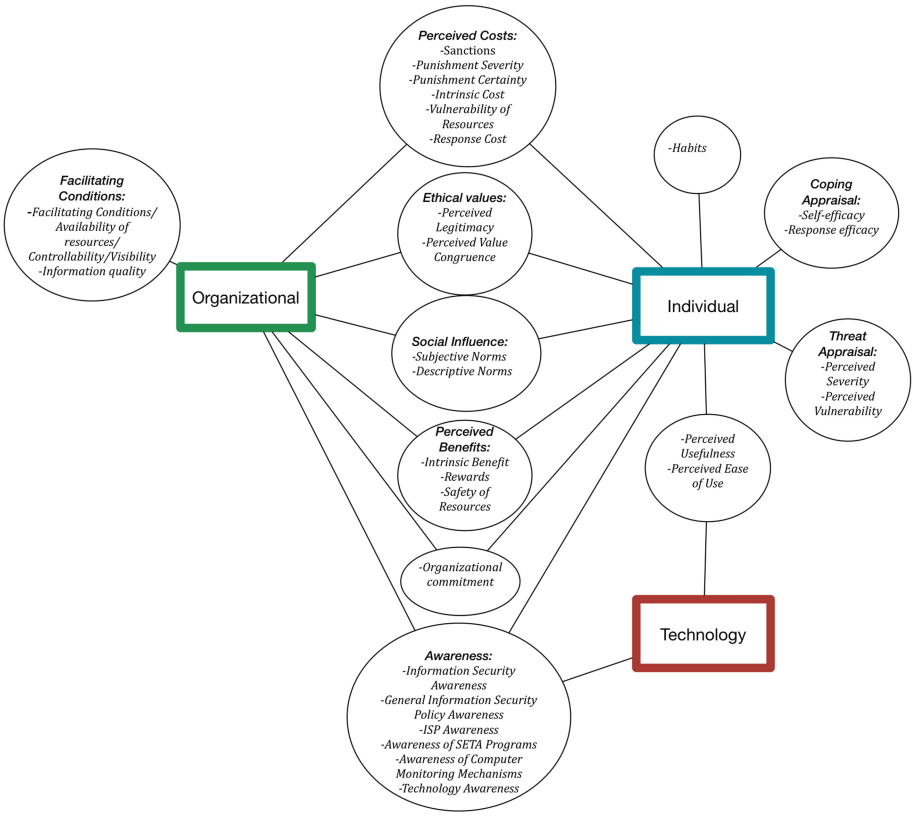

Fig. 1. Individual, organizational, and technical factors influencing security behavior

(self-efficacy) [2, 8, 9, 12, 15, 16, 17]. It is also important to illustrate, possibly through case studies or simulations, the effectiveness of security policies and controls for mitigating security threats and the benefits for the organization and its members *(response efficacy)* [9, 10, 12, 15, 16, 17].

Security awareness is important for security behavior. Furthermore, users' knowledge of the ISPs is also critical [5]. Overall, security education and training awareness programs, enhance individuals' skills to carry out security tasks and foster security compliance [2, 6]. In order to develop a security-oriented culture, security management has to ensure that employees are well informed about the security policies, through awareness and training programs [3] and by employing different communication channels and methods [26].

Security managers should embed security practices and tools into work practices, so as to encourage users to develop security habits [13, 17]. Moreover, these practices and tools need to be seamlessly incorporated into work practices so as to minimize the cost of compliance in terms of effort or time and possible work impediment that negatively influence compliance [5]. It is also important to take into consideration

users' ethical values and beliefs so that employees are convinced that security policies and controls are appropriate, ethical and just [11, 25].

Security management should also emphasize on the positive outcomes that derive from ISP compliance, both for users as well as for organizations [5] and illustrate the negative consequences of non compliance. Rewards, such as pay raises, personal mention, promotions may stimulate security behavior and are worth considering [5, 13, 15, 17]. Sanctions, on the other hand, have not been found to promote compliance. However, the possibility that non compliance is monitored, has been connected with increased compliance [2, 6]. Security management needs to encourage users' daily actions that follow security rules and prohibit employees from habits that may result to security violations (e.g. sharing passwords among colleagues). Additional time and effort for complying with security policies (if required) should be properly explained emphasizing on the benefits of effective security.

3.2 Creating a Facilitating Organizational Setting

Besides individual traits and beliefs, the organizational setting also influences strongly users' security behavior. Thus, security management should create a facilitating environment, by providing users with encouragement, time and the appropriate resources in order to follow ISPs and use security controls [9, 13]. This can be achieved by developing and sharing with users security related material, in the form of campaigns, posters and advertisements through different media [16]. Good quality of this material, as well as clarity and comprehensiveness of the ISP can also promote user compliance [12, 13, 15]. ISPs have to be easily accessible, comprehensible and available in many forms, either printed or in electronic form. Employees should also be aware of computer mechanisms that are implemented, in order to detect security violations [2].

Another important issue for compliance is strong management support, as both organizational commitment [9] and social influence [10] play a critical role in shaping employees' security behavior. Expectations of others, such as colleagues and superiors, have been found to influence users' behavior, towards complying with the ISP [2, 5, 8–10, 13, 16]. At the same time, users tend to replicate the behavior of others [9, 10], which is something that security management should take advantage of. Hu et al. [24] illustrate the importance of the involvement of top management for security compliance. The participation of top management influences organizational culture which in turn influences the employees' attitude towards complying with the ISP. In this way, management influences employees by promoting security compliant behavior, which has been identified as more effective than imposing sanctions and other deterrent mechanisms.

Chipperfield and Furnell [26], report that knowledge about security issues to the employees can be conveyed via "pull" or "push" methods. According to Sommestad et al. [11], organizations should enhance the security compliance of their employees by using "pull" methods, by focusing on the values and emotions of the employees, rather than "push" methods (such as sanctions and rewards). Consequently, security managers should encourage the involvement of the employees in the making of ISPs process and in the creation of a common vision for the organization. As a result employees will be more likely to comply with the ISPs, which will be part of the organizational culture.

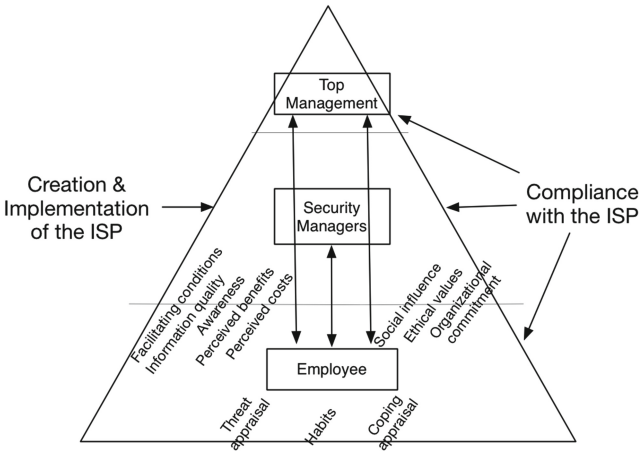

Fig. 2. The influence of organization context on ISP compliance

As depicted in Fig. 2, security managers need to take into consideration different factors that influence employees' security. By applying "pull" methods, that take into consideration the values of the employees and encouraging their involvement in the process of creating ISPs, security managers promote employee compliance and facilitate the development of a security-oriented organizational culture.

3.3 Considering the Technological Aspect

Technological artifacts influence security behavior, as users form expectations with regard to how easy or useful security policies and controls are for them [2, 8]. According to Herath et al. [27], for instance, individuals' intention to use an email authentication service was influenced by the response time of the system (perceived responsiveness). When the service needed long time to check the authenticity of the emails, individuals formed a negative attitude towards its use. Finally, the estimation of the employees' capabilities to identify the malicious emails without using the service was found to influence the intention to use the email authentication service negatively. Payne and Edwards [14], identify usability as an important characteristic of security mechanisms. They report that in many cases authentication and email encryption tools are not used properly or do not gain the approval of users, because of limited user friendliness. Thus, characteristics, such as Revocability, Visibility, Expressiveness, Identifiability etc. should be taken into account when designing security tools and practices.

4 Conclusions and Further Research

This paper analyzes and categorizes factors that influence security behavior as they have been studied in relevant literature. We have identified a large set of factors that are related to individuals (e.g. threat appraisal, coping appraisal, habits), organizational

setting and technology. These factors shape (directly or indirectly) users' intention to comply with a security policy as well as their overall security behavior. The paper provides a complete picture of how security behavior is shaped and gives directions to security managers for identifying and tackling critical issues when creating and implementing security policies so as to foster compliance and promote security behavior.

Furthermore, the analysis of relevant research provides interesting findings with regard to what has not been studied up to now. Though security behavior is found to be influenced by a multitude of organizational factors, the outer context of the environment, e.g. technology, type of business, legal environment have not been examined. The role of technology, in particular, needs further investigation. Research in [8] indicates that individuals tend to adopt a certain protective technology irrespective of how easy it is in use, if they know that there will be severe consequences on their system, in case this technology is not used. It is thus important to enhance our understanding of how technology-related factors influence security behavior so as to employ technical countermeasures that are more appropriate for the organization's function and security protection. This stream of research might also lead to the development of user-friendly security tools.

References

1. Akers, R.: Rational choice, deterrence, and social learning theory in criminology: the path not taken. J. Crim. Law Criminol. **81**, 653 (1990)
2. Al-Omari, A., El-Gayar, O., Deokar, A.: Security policy compliance: user acceptance perspective. In: System Science (HICSS), 45th Hawaii International Conference on System Sciences, IEEE (2012)
3. Albrechtsen, E., Hovden, J.: Improving information security awareness and behavior through dialogue, participation and collective reflection. An invention study. Comput. Secur. **29**(4), 432–445 (2010)
4. Zhang, J., Reithel, B.J., Li, H.: Impact of perceived technical protection on security behaviors. Inf. Manag. Comput. Secur. **17**(4), 330–340 (2009)
5. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34** (3), 523–548 (2010)
6. D'Arcy, J., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. **20**(1), 79–98 (2009)
7. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User acceptance of computer technology: a comparison of two theoretical models. Manage. Sci. **35**(8), 982–1003 (1989)
8. Dinev, T., Hu, Q.: The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. **8**(7), 23 (2007)
9. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**(2), 106–125 (2009)
10. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. **47**(2), 154–165 (2009)

11. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manage. Comput. Secur. **22**(1), 42–75 (2014)
12. Pahnila, S., Karjalainen, M., Siponen, M.: Information security behavior: towards multi-stage models. In: PACIS (2013)
13. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards IS security policy compliance. In: System Sciences 40th Annual Hawaii International Conference on System Sciences, pp. 156b–156b. IEEE (2007)
14. Payne, B.D., Edwards, W.K.: A brief introduction to usable security. Internet Comput. IEEE **12**(3), 13–21 (2008)
15. Siponen, M., Mahmood, A., Pahnila, S.: Employees' adherence to information security policies: an exploratory field study. Inf. Manage. **51**(2), 217–224 (2014)
16. Siponen, M., Pahnila, S., Mahmood, A.: Factors influencing protection motivation and IS security policy compliance. In: Innovations in Information Technology, IEEE (2006)
17. Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manage. **49**(3), 190–198 (2012)
18. Von Solms, R., Von Solms, B.: From policies to culture. Comput. Secur. **23**(4), 275–279 (2004)
19. Vroom, C., Von Solms, R.: Towards information security behavioral compliance. Comput. Secur. **23**(3), 191–198 (2004)
20. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, H.M.: Information security awareness and behavior: a theory-based literature review. Manage. Res. Rev. **37**(12), 1049–1092 (2014)
21. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013)
22. Padayachee, K.: Taxonomy of compliant information security behavior. Comput. Secur. **31**(5), 673–680 (2012)
23. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing employee compliance with information security policies: the critical role of top management and organizational culture*. Decis. Sci. **43**(4), 615–660 (2012)
24. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. **31**(1), 83–95 (2012)
25. Son, J.Y.: Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf. Manage. **48**(7), 296–302 (2011)
26. Chipperfield, C., Furnell, S.: From security policy to practice: sending the right messages. Comput. Fraud Secur. **2010**(3), 13–19 (2010)
27. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R.: Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. **24**(1), 61–84 (2014)