The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/0959-3845.htm

Are users competent to comply with information security policies? An analysis of professional competence models

Aggeliki Tsohou
Department of Informatics, Ionian University, Corfu, Greece, and
Philipp Holtkamp
Department of Computer Science and Information Systems, Jyvaskylan Yliopisto, Jyvaskyla, Finland

Received 16 February 2017
Revised 22 November 2017
Accepted 6 January 2018

Abstract

Purpose – Information security policies (ISPs) are used by organizations to communicate rules on the use of information systems (IS). Research studies show that compliance with the ISPs is not a straightforward issue and that several factors influence individual behavior toward ISP compliance, such as security awareness or individual perception of security threats. The purpose of this paper is to investigate the competencies associated with users' ISP compliance behavior.
Design/methodology/approach – In order to reveal the competencies that are associated with the users' ISP compliance behavior, the authors systematically analyze the ISP compliance literature and the authors develop an ISP compliance competency model. The authors then target to explore if IS users are equipped with these competencies; to do so, the authors analyze professional competence models from various industry sectors and compare the competencies that they include with the developed ISP compliance competencies.
Findings – The authors identify the competencies associated with ISP compliance and the authors provide evidence on the lack of attention in information security responsibilities demonstrated in professional competence frameworks.
Research limitations/implications – ISP compliance research has focused on identifying the antecedents of ISP compliance behavior. The authors offer an ISP compliance competency model and guide researchers in investigating the issue further by focusing on the professional competencies that are necessary for IS users.
Practical implications – The findings offer new contributions to practitioners by highlighting the lack of attention on the information security responsibilities demonstrated in professional competence frameworks. The paper also provides implications for the design of information security awareness programs and information security management systems in organizations.
Originality/value – To the best of the authors' knowledge, the paper is the first study that addresses ISP compliance behavior from a professional competence perspective.

Keywords Competences, Information management, IT policy, Security

Paper type Research paper

1. Introduction

Organizations often rely on technical security solutions to protect themselves against information security threats. However, employing only technical countermeasures appears insufficient for eliminating information security risks; on the contrary, scholars are pointing out that a combination of technical and organizational security controls is imperative (Dhillon and Backhouse, 2001; Bulgurcu *et al.*, 2010; D'Arcy and Herath, 2011; Siponen and Vance, 2010). Toward this direction, information security policies (ISPs) compliance research aims at strengthening the organizational aspect of information security by understanding and revealing the factors that motivate individuals to comply with security policies and guidelines.

ISP compliance research suggests that the information systems (IS) users make own decisions in their everyday tasks about complying, or not complying, with ISPs in order to protect IS resources. For example, Bulgurcu *et al.* (2010) use the neoclassical economics

Information Technology & People
Vol. 31 No. 5, 2018
pp. 1047-1068
© Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-02-2017-0052

rational choice theory (Brennan and Moehler, 2010) and demonstrate that individuals make rational decisions about complying (or not) with security policies, based on the perceived benefits and costs of the compliance/non-compliance behavior (e.g. sanctions). Ng *et al.* (2009) also advocate that end users make a conscious decision to comply (or not comply) with ISPs, based on the way that they perceive benefits and barriers, own efficacy and other parameters. In another example, scholars (Vance *et al.*, 2012; Herath and Rao, 2009; Ifinedo, 2012; Siponen *et al.*, 2010) use Protection motivation theory (Rogers, 1975, 1983) and show that individuals make own assessments in threat situations in order to decide if they think that it is necessary to take actions for protecting information assets by complying with the security policy. In these assessments, people evaluate aspects related to the threat itself, and also to the countermeasures that ISP enforces. Therefore, ISP literature suggests that individuals do not comply blindly with ISPs, but instead they make own assessments and decisions before performing a security behavior with regards to a security policy. However, despite that research studies show that IS users perform own assessments with regards to ISPs, we find no study in IS literature investigating if they are actually prepared to make these assessments and take the associate decisions. In order to further examine this topic, we focus on competence domain, which advocates that competences (i.e. knowledge, skills, and attitudes) that guide human behavior. Therefore, we investigate if IS users actually hold the necessary competencies for making those assessments and decide their security behavior. Examining people's competencies for improving security is also in line with recent guidance given by information security governance frameworks; specifically, ISO 27001 (2013) requires that organizations should determine the necessary competencies of each organizational member that affects the member's information security performance. Similarly, Padayachee (2012) argues that users' motivation is determinant for ISP compliance. Users' competences (i.e. skills and knowledge to maintain security controls) are a key factor which influences users' motivation, thus affecting ISP compliance behavior. Padayachee (2012) argues that the lack of competences is a factor that may result in an end users' failure to recognize the value of security measures. Nonetheless, the literature does not provide any further guidance on the type of competencies that are needed for information security or how to achieve them.

Our research objective is to explore if individuals requested to comply with ISPs are competent to do so. In order to achieve this, we first ask "What competencies are necessary for end users to guide their ISP compliance behavior?" Literature shows that there are several antecedents of individuals' decisions to comply or not with a security policy and we examine what are the competencies associated with them. Additionally, we note that the individuals who are requested to comply with a security policy commonly are professionals in various industry sectors, e.g., human resources professionals, banking professionals, accounting professionals, etc. Given that those are the people who are expected to possess the above competences, we formulate our second research goal as to determine if "ISP compliance competencies are integrated in professional competence frameworks?"

Our analysis leads us to argue that ISP compliance models indeed imply that individuals should acquire security competencies for achieving the desired security behavior (i.e. ISP compliance). We first examined the ISP compliance literature in order to reveal the implications of ISP research for necessary competencies. This process revealed a number of ISP compliance related competences that are either directly associated (e.g. information security awareness) or implied (calculating perceived security threat probability). In order to achieve our second research goal, we examined global professional competence frameworks in various sectors so as to extract if those ISP compliance competencies are taken into account. Based on our findings, professional competence models do not promote the ISP compliance associated competencies. Further, our analysis shows that ISP compliance literature focuses on the antecedents of security behaviors without examining the professional competences surrounding those antecedents. Our study offers new contributions for research and practice, including future research directions and security awareness and management implications.

The paper is structured as follows: the next section presents the theoretical background on understanding competences and Section 3 provides a detailed analysis of ISP compliance literature with regards to competencies. In Section 4, we describe the methodology used to select professional competence frameworks, which we analyze with regards to the findings of Section 3. In Section 5, we discuss our contributions and the research and practical implications that may derive. Section 6 concludes the paper.

2. Background: competency and its effect on individual behavior

On an individual level, competency is used in multiple different disciplines to describe a wide range of characteristics related to job performance (McClelland, 1973). Hereby, job performance is commonly defined as "the total expected value to the organization of the discrete behavioral episodes that an individual carries out over a standard period of time" (Motowidlo, 2003, p. 53). Accordingly, job performance describes behaviors prescribed by the role in the organization (Katz and Kahn, 1978). Thus, competency can be understood as characteristics of an individual directly influencing the behavior. However, so far, no consistent understanding of what these characteristics are and no consistent definition of the term competency exist (Schippmann *et al.*, 2000).

Accordingly, a variety of different approaches co-exist. Commonly, knowledge, skills and abilities are included in these characteristics (Cheney *et al.*, 1990; Winterton, 2009; Boyatzis, 1982). Additionally, other authors include aspects such as motives, traits or attitudes (Spencer and Spencer, 1993) or define competency directly as actual behavior (Dalton, 1997). Other authors address the lack of context specification (Sandberg, 2010) and the lack of target orientation (Boyatzis, 1982). Based on an extensive literature review, Holtkamp *et al.* (2014) define competency as a set of knowledge, skills and attitudes to solve a problem in a given context. The often synonymously used term competence, they defined as single instance of competency and accordingly as a specific knowledge item, skill or attitude necessary to fulfill a single task in a given context. Hereby, knowledge addresses content or technical information that is required to perform a job (Renck *et al.*, 1969), skills refer to psychomotor processes manifested in behaviors (Cheney *et al.*, 1990), and abilities refer to cognitive factors or behaviors that can be seen as the result of personal traits (Renck *et al.*, 1969). Accordingly, abilities are often also referred to as attitudes (Peppard and Ward, 2004).

3. Developing an ISP compliance competency model based on ISP compliance literature

3.1 Selecting the literature

We adopted the guidelines of Webster and Watson (2002) and Von Brocke *et al.* (2009) for a systematic literature review. We targeted quantitative studies that identify determinant factors of ISP compliance behavior published between 2005 and 2016. We used the keywords "information security policy compliance," "security policy violation," "antecedents," "determinant factors," "compliance behavior" and "compliance intention." Following the recommendations of Webster and Watson (2002), we began our investigation with the leading journals of IS, i.e., *European Journal of Information Systems*, *Information Systems Journal*, *Information Systems Research*, *Journal of the AIS*, *Journal of Information Technology*, *Journal of Management Information Systems*, *Journal of Strategic Information Systems* and *Management Information Systems Quarterly*. This investigation led to the selection of nine articles. In sequence we noticed that these nine articles referred to other ISP compliance models, so we went through their reference lists and found eight more articles that included quantitative ISP compliance models. Further, we expanded our research to ACM digital library, Elsevier/ScienceDirect and EBSCOhost (Business Source Premier) information systems and computer science databases using the same keywords. We also searched publications from leading information systems conference proceedings and specifically ICIS, ECIS, AMCIS, PACIS and MCIS, with the same keywords. This led as to additionally include 14 articles. We also took into account the recent systematic review of quantitative studies for ISP compliance by Sommestad *et al.* (2014) which gave us an extra article to analyze.

3.2 Analyzing the ISP compliance literature

Our literature analysis aims to identify the determinant factors that studies include for explaining and predicting ISP compliance behavior. For each of the identified factors, we examined not only how researchers define them based on the construct definitions, but also how they conceptualize them into their survey questions. Through this analysis we revealed the knowledge, skills and attitudes that are implied behind those determinant factors, and therefore the competencies hidden behind ISP compliance behavior and antecedents. Our rationale is that ISP compliance behavior is determined by certain antecedents (e.g. perceived severity of sanctions), and these antecedents are associated with certain competencies, which have not been revealed by information security researchers. We address this gap in this paper by revealing these competencies that are hidden in ISP compliance behavior models.

3.3 Results of literature analysis: the hidden competencies behind ISP compliance

ISP compliance literature presents a rich spectrum of theoretical models explaining the antecedents of individuals' security compliance intention. Common factors identified to determine compliance intention and/or behavior include subjective norms, self-efficacy, response efficacy, response cost, perceived severity of sanctions, perceived certainty of sanctions, perceived probability and perceived severity of security breach, habit and others. In the literature, we can already find studies that summarize those factors (Sommestad *et al.*, 2014; Tsohou *et al.*, 2015). However, what is missing from the literature and is interesting for the purposes of our paper is to analyze the hidden competencies behind these factors.

Starting by the definition of competency, it is clear that it refers to characteristics of an individual associated with his/her performance and refers to specific knowledge, skill or attitudes necessary to fulfill a task belonging to the job (Winterton, 2009). Generally speaking, ISPs request from individuals to perform certain tasks (e.g. locking computer before leaving the desk, applying clear desk practices, selecting strong passwords, and so on) and failure to complete these tasks may lead to sanctions. Therefore, the context itself leads us to the conclusion that ISP compliance is associated with certain individuals' competencies. In this section, we will demonstrate that ISP compliance theories also lead us to the same conclusion. Lin and Kunnathur (2013) have made a first attempt to demonstrate this argument and present a framework of end-user security competencies. In this section, we elaborate on the antecedents of ISP compliance behavior, taking into account not only the construct definition but also the understanding of each factor by analyzing the survey instruments and associated questions. Using the outcomes of this analysis, we formulate the basis for our competency framework.

3.3.1 Directly mentioned competencies. 3.3.1.1 Attitude toward compliance with the ISP. We begin our presentation with the most obviously stated information security competence: attitude toward ISP compliance. Bulgurcu *et al.* (2010) identifies this as a distinct construct influencing individuals' intention to comply and defines it as "the degree to which the performance of the compliance behavior is positively valued." The study measures the factor through the opinion of individuals regarding the need to comply with the requirements of the ISP (i.e. necessary/unnecessary, beneficial/unbeneficial, important/unimportant and useful/useless). Similarly, Aurigemma and Mattson (2014) and Al-Omari *et al.* (2012) conceptualize attitude related to the person's overall evaluation of desirability and positive evaluation of implementing the ISP compliance behavior, expressed through questions regarding how important, helpful, exciting and beneficial the security controls are.

We argue that attitude inclined toward compliance to ISP is a directly mentioned competence. Competency definitions include attitude complementary to knowledge and skills because competency is closely related to behavior; having the right skills, but the wrong attitude does not lead to the expected behavior. An indicative competency associated with this construct of ISP compliance models is an individual's "positive attitude towards security compliance."

3.3.1.2 Information security awareness and training. Information security awareness has been assumed (Yang *et al.*, 2011) and validated as a determinant factor of ISP compliance intention (Haeussinger and Kranz, 2013; D'Arcy *et al.*, 2009; Bulgurcu *et al.*, 2010; Talib and Dhillon, 2015; Putri and Hovav, 2014; Al-Omari *et al.*, 2012; Merhi and Midha, 2012), directly or indirectly. Bulgurcu *et al.* (2010), Haeussinger and Kranz (2013) and Al-Omari *et al.* (2012) differentiate two types of awareness: general security awareness and ISP awareness. General security awareness involves an understanding of security threats and their consequences, an understanding of concerns and risks, and knowledge about the cost of potential security problems (Bulgurcu *et al.*, 2010, p. 536). Equally, the lack of ISP knowledge and understanding of ISP has been validated as a factor influencing intention to violate a policy (Siponen and Vance, 2010). ISP awareness refers to knowledge and understanding of ISP rules, as well as resulting responsibilities. D'Arcy *et al.* (2009) also examine ISP awareness defined as awareness of ISP guidelines and rules. Therefore, we argue that both types of awareness are directly mentioned competencies. Indicatively, these competencies refer to an individual's "knowledge of ISP rules" and "knowledge of the value of information security for the organization."

3.3.2 Implied competencies. 3.3.2.1 Perceived rewards/sanctions. Rewards, as an antecedent of ISP compliance, are conceptualized as the perception of an employee for pay raises, promotions, monetary rewards, or intangible rewards that may result from ISP compliance (Bulgurcu *et al.*, 2010). Similarly, sanctions as a construct is understood as the perceived punishments, demotions, reprimands, monetary or non-monetary penalties and other tangible or intangible sanctions that may result from ISP non-compliance (Bulgurcu *et al.*, 2010; Siponen and Vance, 2010; Kirsch and Boss, 2007). Therefore, research models conceptualize both concepts as the understanding of an individual about the reward and sanction associated with ISP compliance behavior. Literature shows that when individuals are aware of punishments that will follow undesirable behaviors, they are less likely to commit a deviant act (Chen *et al.*, 2012). Vance and Siponen (2012) differentiate between formal and informal sanctions upon ISP non-compliance and although they assumed a significant correlation between sanctions and ISP compliance intention, their research did not find support on this. Aurigemma and Mattson (2014) and Merhi and Ahluwalia (2014) find significant relationship between both severity and certainty of sanctions and intention to comply with ISP. Further research demonstrates that rewards are important for promoting compliance behaviors (Chen *et al.*, 2012; Kirsch and Boss, 2007).

We argue that there are competences hidden behind an individual's understanding of rewards and sanctions associated with ISP compliance, which is implied by the way the constructs are measured. In particular, it implies that the individuals have the knowledge of the ISP existence and content. Further, it implies that the individual has the ability to understand which rule of the ISP applies every time and the ability to recognize which actions fall under the ISP. As an indicative example, we may consider an ISP that forbids employees to perform any illegal activities within the organizational network or through the organizational IT devices. Now let us consider an employee who aims to install a torrent client in a work laptop. For the employee to realize that a sanction would be connected with installing the torrent client, the employee should not only have the knowledge of the ISP rule (i.e. knowledge), but also she(he) should possess the ability (i.e. skills) to identify that the torrent installation is an illegal activity through organizational IT devices.

3.3.2.2 Self-efficacy. ISP research validates that perceived self-efficacy is a determinant factor for ISP compliance intention; when individuals are requested to use a specific safeguard (e.g. an antivirus software), they evaluate their own ability to use the safeguard. Self-efficacy refers to the individual's belief regarding how easy it would be for them to use the security control, how effortless, and how convenient it will be (Johnston and Warkentin, 2010; Johnston *et al.*, 2015; Wall *et al.*, 2013; Al-Omari *et al.*, 2012). Additionally, earlier models like Kirsch and Boss (2007) verify that computer self-efficacy determines if individuals will adopt security controls to protect information assets. Computer self-efficacy in that study means that the individual needs help by another person in order to complete their job using a software package used for the purposes of the study.

We argue that this construct also implies that applying the ISP requires the user to possess certain knowledge and skills for using the associated control. As an indicative example, we may consider an ISP that obliges employees to encrypt any file that includes personal data before sending it via e-mail to anyone. Self-efficacy in this example means that the employee should assess her own knowledge regarding the use of encryption tools. The employee should also assess her own ability to recognize a file that should be sent encrypted from another file that should be sent unencrypted (i.e. a file that contains personal data from a file that does not contain personal data). An indicative implied competency, thus, is not only an individual's "knowledge for applying encryption," but also "the ability to recognize when a file contains personal data."

3.3.2.3 Perceived cost of compliance/perceived benefit of compliance. Researchers identify perceived cost and benefit of compliance as two factors influencing ISP compliance behavior (Vance *et al.*, 2012; Ifinedo, 2012; Bulgurcu *et al.*, 2010). This means that ISP compliance behavior is associated with how individuals assess the cost and benefit of compliance. For example, Bulgurcu *et al.* (2010) measure the benefit as the individual's perception of compliance bring advantages, benefits, gains and being favorable. The cost is measured as the individual's perception of compliance as time consuming, overhead loading, inconvenient, burdensome and costly for him/her (Bulgurcu *et al.*, 2010; Vance *et al.*, 2012; Ifinedo, 2012; Putri and Hovav, 2014). Work inconvenience (Bulgurcu *et al.*, 2010) sometimes is even differentiated from the other cost implications. Further, Vance *et al.* (2012) discuss the role of rewards as perceived time savings.

We argue that assessing the costs and benefits of compliance implies that the individual has a certain set of skills that allow him/her to perform such assessments. As an example, we can consider the case of an ISP that obliges employees to enable a VPN connection when using the internet from organizational IT devices outside the company. Let us also assume that the rule is not technically enforced (thus an employee can still use online services without VPN connection). According to ISP compliance models, the employee will evaluate if connecting through VPN creates a large overhead and inconvenience to her, and what would be the benefit from complying with the rule, before deciding if she(he) will comply with the ISP. This implies that the employee not only has the "ability to assess when and for what reasons to set a VPN connection" but also "the ability to evaluate the burden created by setting up the VPN connection."

3.3.2.4 Perceived severity and perceived certainty of sanctions. Sanctions are associated not only with the knowledge of their existence (i.e. if users know the sanctions that will be enforced in case on ISP non-compliance), but also with personal assessments regarding sanctions' certainty and severity (Johnston *et al.*, 2015; Aurigemma and Mattson, 2014; Merhi and Ahluwalia, 2014; Li *et al.*, 2010). Further, the type of the sanctions (formal or informal) is associated with ISP compliance behavior. Similarly to the previous constructs, we argue that this construct implies that employees should possess competencies related to understanding the probability and certainty of sanctions. As an indicative example, we can imagine an ISP that forbids employees to use social media during working hours. Let us imagine the situation in which an employee considers to post a message on Facebook using a work laptop, a work desktop computer, a personal tablet, or a personal smartphone. First, the employee would need to understand which one of the above cases is a violation of the ISP. For example, is the behavior of posting a message on Facebook through personal smartphone and own mobile data bandwidth a violation of the ISP? Second, the employee would need to assess what is the probability that the organization would find out about the violation for each case and whether the sanction would be different depending on the case.

3.3.2.5 Perceived threat probability, vulnerability and severity of security breach. ISP literature demonstrates that individuals' intention to conform to an ISP depends on their own risk assessment of the threat and vulnerability associated to a particular control (Johnston and Warkentin, 2010; Putri and Hovav, 2014). Assessing threat severity means that the individual estimates if the threat would be severe, serious and significant for a particular IT asset.

Perhaps, this is the most striking example of ISP compliance determinants related to competencies. Assessing threat probability means that the individual makes an estimation of how likely and probable it is that the particular IT asset would be the target of a threat. We argue that assessing the threat probability and severity implies that the IS users have certain skills that allow them to do so. For example, we may consider an ISP that obliges IT administrators to keep a daily data backup in a different location than the computer room. The IT administrator would assess the possibility of a fire or a flooding, before complying with the rule. Our argument is that this involves skills that should be fostered through threat appraisal training, i.e., "training to empower employees to be able to assess threats, understand threats severity as well as the likelihood of its occurring" (Merhi and Midha, 2012).

3.3.2.6 Response efficacy. Behavioral models validate that SI users' judgment of the ISP is influential for their compliance behavior. In particular, policy efficacy has been identified as a determinant factor of ISP compliance intention and refers to the individuals' assessment about the effectiveness of a control against a security threat (Johnston and Warkentin, 2010; Johnston *et al.*, 2015; Putri and Hovav, 2014). As an example, we may consider an ISP that enforces password protection on any USB storing organizational information. Let us imagine a manager who has heard many stories about how easy it is for an expert attacker to overpass a password. According to the ISP compliance models in the literature, the manager will be inclined toward incompliance to the ISP because she(he) perceives that the particular security control is not efficient (i.e. perceived weak control efficacy). However, the company may have enforced the particular control in the ISP in order to reduce the risk of accidental data disclosure, and not the intentional data disclosure following an attack by a knowledgeable expert. Thus, response efficacy implies that individuals have the "ability to evaluate the effectiveness of security controls" in particular contexts/situations.

3.4 A proposed ISP compliance competency model

Following our analysis of the ISP compliance literature, we can conclude that scholars reveal the antecedents of ISP compliance behavior. Whether IS users will comply with ISPs is affected by numerous factors, including how they assess a security threat severity, how they estimate their own efficacy in applying the recommended security controls, the existence of habits and other factors. Through our analysis of the ISP compliance models, we can recognize specific antecedents of ISP compliance behavior that either constitute a professional competence themselves (direct competences) or imply a hidden competence for the IS user (implied competences). Based on our analysis, we develop an ISP compliance competence model presented in Table I. Table I also presents the associated antecedents in ISP literature and their descriptions.

We argue that an expression of the associated competencies requires further investigation using empirical data in organizational settings and variety of ISPs. The utilization of

Competence dimension	ISP compliance factor	Description of competence	References
Attitudes	Attitude toward ISP compliance	Personal stance against ISP compliance	Bulgurcu *et al.* (2010), Aurigemma and Mattson (2014), Al-Omari *et al.* (2012)
Skills	Perceived rewards	The individual's personal assessment of perceived time savings	Vance *et al.* (2012)
	Perceived cost	The individual's personal assessment of the time, overhead, inconvenience, work impediment, burden resulting from compliance behavior	Vance *et al.* (2012), Ifinedo (2012), Bulgurcu *et al.* (2010), Putri and Hovav (2014)
	Perceived benefit	The individual's personal assessment of the gains, advantages, and benefits, resulting from compliance behavior	Bulgurcu *et al.* (2010)
	Perceived threat probability and severity	The individual's personal assessment of the threat likelihood, severity and vulnerability levels	Johnston and Warkentin (2010), Johnston *et al.* (2015), Putri and Hovav (2014), Merhi and Midha (2012)
	Perceived control efficacy	The individual's personal assessment of the effectiveness of the control for protecting against a threat	Johnston and Warkentin (2010), Johnston *et al.* (2015), Putri and Hovav (2014)
	Perceived severity and certainty of sanctions	The individual's personal assessment of the likelihood that sanctions will be applied in case of incompliance, the speed of the enforcement and the severity of them	Johnston *et al.* (2015), Chen *et al.* (2012), Aurigemma and Mattson (2014), Merhi and Ahluwalia (2014), Li *et al.* (2010)
	Perceived self-efficacy	Skills that allow using a certain information security control or technology	Johnston and Warkentin (2010), Johnston *et al.* (2015), Kirsch and Boss (2007), Al-Omari *et al.* (2012)
Knowledge	General security awareness	Knowledge about the cost of potential security problems	Bulgurcu *et al.* (2010), Haeussinger and Kranz (2013), Al-Omari *et al.* (2012)
	ISP awareness	Knowledge and understanding of ISP rules	Bulgurcu *et al.* (2010), Haeussinger and Kranz (2013), D'Arcy *et al.* (2009), Siponen and Vance (2010), Yang *et al.* (2011), Talib and Dhillon (2015), Putri and Hovav (2014), Al-Omari *et al.* (2012), Merhi and Midha (2012)
	Perceived self-efficacy	Knowledge that allows using a certain information security control or computers	Johnston and Warkentin (2010), Johnston *et al.* (2015), Kirsch and Boss (2007)
	Perceived rewards	Knowledge of monetary or other rewards given by the organization in case of compliance	Bulgurcu *et al.* (2010), Chen *et al.* (2012), Kirsch and Boss (2007)
	Perceived sanctions	Knowledge of monetary or other sanctions given by the organization in case of non-compliance	Bulgurcu *et al.* (2010), Chen *et al.* (2012), Kirsch and Boss (2007)

Table I.
Competences in ISP compliance models

competence theories would also be encouraged (see Section 5.1) for proposing a complete competency model. Nonetheless, we describe in Table II a set of indicative competencies that derive from the analysis of the literature.

It is worth mentioning that Table I presents the research constructs as found in the ISP compliance literature and Table II presents indicative examples of competencies. One observation is that the respective competencies are also safeguard specific (e.g. ability to assess the efficacy of antivirus, knowledge of smartcard usage for authorization, ability to assess the burden resulting from mobile device locking and tracking). For example, an employee requires different knowledge and skills in order to assess the level of a network intrusion threat (i.e. perceived threat probability and severity) compared to the knowledge and skills required to assess the level of a social engineering threat. This has been properly highlighted in the literature by Siponen and Vance (2010), who manipulated their survey with regards to three safeguard scenarios (i.e. USB drive protection, workstation logout, and password protection). Perhaps, the most striking example on the importance of this remark refers to the self-efficacy factor. Self-efficacy refers to the individual's belief on how easy it would be for them to use the safeguard, how effortless, and how convenient it will be. If we imagine the multitude of safeguards that an ISP includes, we can understand that knowledge and skills that are hidden behind self-efficacy are safeguard specific.

4. An analysis of competence frameworks with "an eye" on ISP compliance competencies

4.1 Selecting the frameworks

Our research proceeds with identifying the extent to which the competencies underlying commonly used models for security compliance are taken up in practice. To do so, we analyzed the extent to which the competencies that we revealed (Table I) are represented in professional competency frameworks. A vast amount of different competency frameworks in organizational, industry sectorial and profession-level practice and literature can be found. To ensure a rigorous selection and exclude company/industry specific regulations, we focused on professional-level competence frameworks. Furthermore, to exclude national and cultural aspects, we focused only on competence frameworks published by international associations. We focused on professions that commonly entail high IT usage without, however, being IT professionals. In total, eight different competence frameworks were analyzed. These frameworks address competency requirements for project management, human resource management, facility management, accounting, and administration professionals. As our analysis proceeded (see the next section), the eight competence frameworks provided a very coherent picture and no big differences, while no new findings are expected from additional frameworks,

Competence dimension	Indicative competencies
Attitudes	Positive attitude toward security compliance
Skills	Ability to assess the situations in which ISP rules apply
	Ability to assess own knowledge for applying security controls
	Ability to assess burden from security controls
	Ability to assess the benefits of security controls
	Ability to assess security threat likelihood, threat severity and vulnerability
	Ability to evaluate the effectiveness of security controls
	Ability to assess the probability and severity of sanctions
Knowledge	Knowledge about the cost of potential security problems
	Knowledge of ISP rules
	Knowledge of applying a security control

Table II.
An indicative ISP compliance competence model

i.e., saturation. For this reason, the eight frameworks that we analyzed were considered as sufficient evidence for our research goals. For the detailed analysis, please see Table AI. Next, we provide a description of the findings.

4.2 An analysis of the frameworks: IT and security competences

Project management frameworks include some competences that are associated with IT knowledge and skills. For example, Project Management Competency Framework (PMCF, 2007) suggests that project management professionals should be able to select tools for communication and tools for project management. The framework also incorporates competencies for the appropriate use of information sources. Finally, it recommends that professionals should insist on compliance with processes, procedures and policies. The Framework by the Association for Project Management incorporates a more detailed analysis of IT-related competences for project managers, including the knowledge of tools and techniques to perform project management activities (e.g. scheduling, budgeting and others), as well as for stakeholders' communication. In several cases, the framework includes competencies regarding specific technologies, such as budget tracking systems, network diagrams for resource planning, and scheduling tools.

Human resources frameworks incorporate several competencies that are directly associated with technology and IT. For example, the framework by the Society for Human Resource Management (SHRM, 2012) includes the competence to maintain up-to-date knowledge of human resources technology, to use human resources IT systems, to use analytic tools for data gathering and analysis and to utilize social media systems. Also, it involves competencies that imply the use of technology, such as providing clear information in electronic communication. The framework by the Human Resources Professionals Association (HRPA, 2014) recognizes technological savvy (i.e. making use of various technologies to best advantage, seeing the possibilities in emerging technologies and managing the implementation of new technologies) as an enabling competency across all human resources functions. HRPA (2014) includes also other IT-related competences, such as identifying risks associated with technological forces and using human resources tools for maintaining information.

Facility management associations have also published competency frameworks to diffuse global facility management practices and assist professionals' self-assessment for certifications. The International Facility Management Association (IFMA, 2016) holds a competency framework designed for the IFMA's certification process for facility managers covering eleven competencies. IFMA (2016) reveals significant emphasis on information technology competencies. Not only the framework does identify several IT-related competences, such as the competency to collect, verify, analyze and report facility management data, but also dedicates one competency regarding technology, which covers the use and application of technology for facility management.

The International Association of Facilitators (IAF, 2015) promotes six competency areas including limited and indirect references to information technology skills, knowledge and attitudes. Specifically, it only refers to the competence of identifying information associated with the tasks in question and drawing out data.

The International Association for Administrative Professionals (IAAP, 2016) provides a set of competencies comprising seven domains also associated with a relevant professional certification. The framework identifies several IT-related competencies, such as the knowledge of software applications for business documents and spreadsheets, the knowledge of software that is appropriate for office design and publishing, online tools for web publishing, and software applications that are appropriate for compiling, storing and analyzing data. Additionally, it covers knowledge on the use of e-mail, social media and internet, as well as knowledge of software, systems and services for electronic filing.

In addition to IT competencies, we were also interested in identifying competencies included in the professional frameworks that relate to information security. In particular, we were interested in identifying any competencies that are related to our proposed ISP compliance competency model (depicted in Table I). For only few cases we found such competencies, and in other cases we identified competencies that could be associated with information security. The Competency Model by the Society for Human Resource Management (SHRM, 2012) is a competency model on Ethical Practice; individuals at the highest level of proficiency on this competency are expected to "Create processes to ensure confidentiality and privacy of employee information and company data." In most cases, the competency frameworks included knowledge, skills or attitudes associated with the development and application of organizational processes, procedures and policies (PMCF, 2007; SHRM, 2012; HRPA, 2014). In that sense, we can assume that those competencies may also refer to ISPs, although they are not information security specific ones. A striking example covering significant competencies on information security is the IFMA (2016) framework, which includes several performances associated to information security, such as the performance of securing technology systems and services, and the selection of security measures that meet the facilities' needs. In terms of ISP compliance though, the competencies are again limited to performances associated to the compliance with codes, regulations, policies and standards. IAAP (2016) also includes competencies associated to organizational information security expected by administration professionals, such as knowledge of security procedures involved in maintaining, backing up, and storing information, and the skill to identify and describe the appropriate security for both electronic and manual files.

Next, we summarize our findings from the analysis of the professional competency models and we discuss their implications.

5. ISP compliance competencies: new contributions for research and practice

In order to explore what are the necessary competencies for ISP compliance, we analyzed existing ISP compliance theories and determined an ISP compliance competency model. The IS stakeholders that are required to comply with ISPs are individuals of various professions and organizational roles. Therefore, one would expect that professional competence frameworks would promote IT and ISP compliance competencies. In order to explore if competency frameworks do so, we analyzed recognized competence schemes with the "eye" to IT and security competences. Our findings indicate the existence of a research and practice gap: on the one hand, ISP compliance research implies that IS users perform activities that require certain competencies, but on the other hand competency frameworks in various professions do not promote those ISP compliance competencies. IS literature also lacks studies explaining what are the information security competencies that non-IT personnel should acquire. Therefore, our findings offer new contributions and implications for research and practice, which we analyze next in detail.

5.1 Research contributions and implications

The analysis of ISP compliance research shows that the majority of research models and theories implicitly assume a set of competencies. However, these competencies are not addressed, or are just rudimentary addressed, by existing professional competency frameworks. Accordingly, the underlying competencies are not reflected in the competency organizational management processes, and especially in the main sources that organizations use to determine necessary personnel competences—that is the professional competency models. Following this, further research is needed to analyze ISP compliance from a competence perspective.

As our findings of the literature review demonstrate, ISP compliance theories commonly have implicit assumptions for competencies and Table II presents indicative examples of such competencies. Further research exploration is necessary on the theoretical foundations that can help researchers better understand the competencies that are involved in ISP compliance behavior. Understanding the underlying competencies holistically (i.e. knowledge, skills and attitudes) may become the key in dealing with the knowing-doing gap that has been widely reported by researchers and practitioners (Martin, 2014; Pfeffer and Sutton, 1999). The knowing-doing gap refers to the situation in which individuals know what they are supposed to do, but do not turn this knowledge into action/behavior. One recommendation toward this direction is the utilization of the competence performance theory (CPT) (Korossy, 1997, 1999). CPT describes how a set of competencies is directly related to a task. According to the theory, competencies directly affect the performance of individuals and their behavior. Performance refers to the empirically observable solution behavior on certain given problems. Competencies are the theoretically founded entities accounting for the observable solution behavior. CPT calls the formal mathematical representations of performances as performance space, the competencies as competence space, and tasks as task space. Based on CPT, top management should connect a competence space with a task space. The theory assumes that an individual who has the competencies in the competence space can perform the task in the associated task space. Therefore, further research using CPT can offer significant insights on how the competencies that we identified in the ISP compliance competency model (Table I) affect the security behavior of individuals. This can be achieved by defining both competence space and task space, associated with the ISP compliance behavior that is expected by employees.

Furthermore, any competency framework requires to be aligned with organizational structure and organizational roles. Following the identification of the relevant and underlying competencies of ISP compliance, another important aspect for further research is to identify factors which are associated with the different roles within an organization. It can be expected that different roles and positions in an organization require different security competencies. Such analysis would be highly valuable for the different professional competences because it can result in the refinement of competency frameworks with the security competences that are necessary in today's organizations, where IS are used in the everyday work practices.

Another relevant future research aspect is the analysis of reasons behind the lack of security-related competences in the competency frameworks. The lack of security competences in the analyzed frameworks is surprising, as the security threats related to human behaviors are increasing drastically for organizations and their business. Furthermore, the role of the IS users with today's modern technologies and blending of personal/professional tasks is becoming increasingly more significant. The important question to answer by further research is whether the lack of these competencies is rooted in the lack of awareness of the importance of security compliance, or on a lack of perceived importance, or on the lack of understanding how security compliance can be reached, or other reasons.

5.2 Managerial and practice contributions and implications

This paper and the findings of our research can offer significant contributions for information security managers, and particularly for the development of security awareness and training programs in organizations. Awareness and training programs are widely used to make IS stakeholders aware of security issues and policies, while training sessions enhance the development of security skills and competences. (ENISA, 2010; NIST 800-50, 2003). There are available guides focusing on the design, implementation and evaluation processes, as well as the security content and communication mechanisms to be used within awareness and training programs. However, literature misses a systematic way to plan awareness and training programs based on targeted behavior and expected results. Information security awareness has been associated with altering and guiding individual behavior (Chen *et al.*, 2006; Parsons *et al.*, 2014; Puhakainen and Siponen, 2010), and for empowering the end users with knowledge and skills that strengthen their motivation to comply with ISPs (Padayachee, 2012). Nonetheless, research is needed to determine the connection of how awareness initiatives will actually result to changes in security behavior (Tsohou *et al.*, 2015). We argue that the competencies behind ISP compliance are the key for addressing this gap. Information security managers can define the ISP compliance competencies that are desirable; knowing what the desirable competencies can assist the awareness and training developers to make justified and targeted decisions, such as security content, delivery channels, group segregation, and so on. Toward this direction, in this paper, we provide an indicative set of ISP compliance competencies (Table II). Information security awareness initiatives would be important for stimulating end users' attitudes, while information security training can offer security behavior specific knowledge and skills to improve targeted antecedents of ISP compliance behaviors, such as self-efficacy. Our study urges information security managers to design control-specific information security awareness and training programs instead of generic ones which is the common practice nowadays. In light of our findings, information security managers can be guided for the contents of awareness and training programs. For example, one of the competencies that we identify in Table II is the "Ability to assess own knowledge for applying security controls." Thus, we recommend information security managers to strengthen employees' understanding of their own knowledge to apply a particular security control. This could be performed via self-assessment methods or other forms of periodic tests. By adopting such practices, managers would ensure that individuals do not underestimate or overestimate their ability to apply a particular security control, which would lead them to incorrect decisions regarding ISP compliance.

Our findings can also assist information security managers, aiming to apply recommended best practices for information security governance or to conform to international standards and become certified for security management processes. ISO 27001 (2013) requests that organizations determine the necessary competences of employees that affect their information security performance. ISO 27002 (2013) requests organizations to make sure that individuals appointed with responsibilities in the information security area are actually competent to fulfill those responsibilities. Our findings from analyzing professional competence models suggest that there is a lack of organizational management knowledge in this area and we provide directions for future actions that can assist bridging this gap.

Further, information security risk assessment is a common practice nowadays for determining information security requirements in an organization (E&Y, 2015; ISO 27005, 2011). During risk assessment, it is imperative that the risk analysts receive the views of all organizational members and interested parties as an important input in order to determine threat and vulnerability levels and perform impact assessments. Our analysis shows that the competencies associated with individuals' perceived threat probability and severity are largely unknown. Gaining an understanding on this aspect and taking actions to ensure that individuals can acquire these necessary competencies can enhance the effectiveness of information security risk assessments for determining security requirements of IS.

6. Conclusions

ISP compliance has received great attention by organizations, especially given that information security breaches caused by human threats are common. In today's consumerization era, in which personal and professional IT of end users are blended

(Gannon, 2013), the end users have a strong role in protecting information security in organizations. A wide stream of research explains individual behavior with regards to ISP compliance and identifies the factors that influence compliance and non-compliance behaviors. In this paper, we take into account these factors and we reveal what competencies are associated with users' decisions about complying or not with a security policy. Based on our analysis, we also offer an indicative ISP compliance competency framework. Having those competencies identified, we also examined if top management had paid attention to those competencies when shaping the profile of their employees in the various professions.

We selected eight professional competence frameworks, with criterion to be published by international associations covering different professions, including project management, human resource management, facility management, accounting, and administration professionals. We focused on professions which commonly have a high IT usage without being IT professionals. Our findings suggest that, on the one hand, ISP compliance theories imply that users perform activities that require certain competencies, but on the other hand, professional competence frameworks do not recommend those competencies. We argue that this is an important research and practical gap with significant implications and we offer directions for future research that can guide managers toward improving their information security awareness programs and information security management systems.

References

Al-Omari, A., El-Gayar, O.F. and Deokar, A.V. (2012), "Information security policy compliance: the role of information security awareness", *Proceedings of the 18th Americas Conference on Information Systems, Seattle, WA, August 9-12*.

Aurigemma, S. and Mattson, T. (2014), "Do it OR ELSE! Exploring the effectiveness of deterrence on employee compliance with information security policies", *Proceedings of the 20th Americas Conference on Information Systems, Savannah, GA, August 7-9*.

Boyatzis, R.E. (1982), "The competent manager: a model for effective performance", *Strategic Management Journal*, Vol. 4 No. 4, pp. 385-387.

Brennan, G. and Moehler, M. (2010), "Neoclassical economics", in Bevir, M. (Ed.), *Encyclopedia of Political Theory*, Vol. II, Sage Publications, Thousand Oaks, CA, pp. 946-951.

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

CGMA (2014), "CGMA competency framework", Chartered Global Management Accountant, Chartered Institute of Management Accountants and the Association of International Certified Professional Accountants, Durham, available at: www.cgma.org/Resources/Tools/DownloadableDocuments/competency-framework-complete.pdf (accessed February 13, 2017).

Chen, C.C., Shaw, R.S. and Yang, S.C. (2006), "Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system", *Information Technology Learning and Performance Journal*, Vol. 24 No. 1, pp. 1-14.

Chen, Y., Ramamurthy, K. and Wen, K. (2012), "Organizations' information security policy compliance: stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157-188.

Cheney, P.H., Hale, D.P. and Kasper, G.M. (1990), "Knowledge, skills and abilities of information systems professionals: past, present, and future", *Information & Management*, Vol. 19 No. 4, pp. 237-247.

D'Arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, Vol. 20 No. 6, pp. 643-658.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Dalton, M. (1997), "Are competency models a waste?", *Training and Development*, Vol. 51 No. 10, pp. 46-49.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: toward socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

E&Y (2015), "Creating trust in the digital world, EY's global information security survey", available at: www.ey.com/publication/vwluassets/ey-global-information-security-survey-2015/$file/ey-global-information-security-survey-2015.pdf (accessed February 13, 2017).

ENISA (2010), "The new users' guide: how to raise information security awareness", available at: www.enisa.europa.eu/publications/archive/copy_of_new-users-guide (accessed February 13, 2017).

Gannon, B. (2013), "Outsiders: an exploratory history of IS in corporations", *Journal of Information Technology*, Vol. 28 No. 1, pp. 50-62.

Haeussinger, F. and Kranz, J. (2013), "Information security awareness: its antecedents and mediating effects on security compliant behavior", *Proceedings of the International Conference on Information Systems ICIS 2013, Milan*.

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

Holtkamp, P., Lau, I. and Pawlowski, J.M. (2014), "How do software development competences change in global settings – an explorative study", *Journal of Software: Evolution and Process*, Vol. 27 No. 1, pp. 50-72.

HRPA (2014), *Human Resources Professional Competency Framework*, Human Resources Professionals Association, Toronto, Ontario, available at: www.hrpa.ca/Documents/…/HRPA-Professional-HR-Competency-Framework.pdf (accessed February 13, 2017).

IAAP (2016), "IAAP Certified Administrative Professional (CAP) exam 2016 body of knowledge", available at: www.iaap-hq.org/page/BOK (accessed February 13, 2017).

IAF (2015), *Core Facilitator Competencies*, International Association of Facilitators, Ontario, available at: www.iaf-world.org/site/professional/core-competencies (accessed February 13, 2017).

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

IFMA (2016), "Complete list of competencies covered on the IFMA CFM exam", available at: www.ifmacredentials.org/cfm/cert-and-recert (accessed February 13, 2017).

ISO 27001 (2013), *Information Technology – an Security Techniques – an Information Security Management Systems – an Requirements*, International Organization for Standardization, Geneva.

ISO 27002 (2013), *Information Technology – an Security Techniques – an Code of Practice for Information Security Controls*, International Organization for Standardization.

ISO 27005 (2011), *Information Technology – an Security Techniques – an Information Security Risk Management*, International Organization for Standardization.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors", *Management Information Systems Quarterly*, Vol. 34 No. 4, pp. 549-566.

Johnston, A.C., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric", *Management Information Systems Quarterly*, Vol. 39 No. 1, pp. 113-134.

Katz, D. and Kahn, R.L. (1978), *The Social Psychology of Organizations*, Wiley, New York, NY.

Kirsch, L. and Boss, S. (2007), "The last line of defense: motivating employees to follow corporate security guidelines", *Proceedings of the International Conference of Information Systems, Montreal, December 9-12*.

Korossy, K. (1997), "Extending the theory of knowledge spaces: a competence-performance approach", *Zeitschrift fur Psychologie*, Vol. 205 No. 1, pp. 53-82.

Korossy, K. (1999), "Modeling knowledge as competence and performance", in Albert, D. and Lukas, J. (Eds), *Knowledge Spaces: Theories, Empirical Research, and Applications*, Psychology Press, Oxford, pp. 103-132.

Li, H., Sarathy, R. and Zhang, J. (2010), "Understanding compliance with internet use policy: an integrative model based on command and control and self-regulatory approaches", *Proceedings of the 31th International Conference on Information Systems, MO, December 12-15*.

Lin, C. and Kunnathur, A.S. (2013), "Toward developing a theory of end user information security competence", *Proceedings of 19th Americas Conference on Information Systems, Chicago, IL, August 15-17*.

McClelland, D. (1973), "Testing for competence rather than for 'intelligence' ", *American Psychologist*, Vol. 28 No. 1, pp. 1-14.

Martin, J. (2014), *Cybersecurity Awareness is About Both "Knowing" and "Doing"*, Cybersecurity Intelligence, IBM, New York, NY, available at: https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/

Merhi, M. and Ahluwalia, P. (2014), "The role of punishment and task dissonance in information security policies compliance", *Twentieth Americas Conference on Information Systems, Savannah, GA, August 7-9*.

Merhi, M. and Midha, V. (2012), "The impact of training and social norms on information security compliance: a pilot study", *Proceedings of the 33rd International Conference on Information Systems, Orlando, FL, December 16-19*.

Motowidlo, S.J. (2003), "Job performance", in Borman, W.C., Ilgen, D.R. and Klimoski, R.J. (Eds), *Handbook of Psychology*, Wiley, London, pp. 39-52.

Ng, B., Kankanhalli, A. and Xu, Y. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825.

NIST 800-50 (2003), "Building an information technology security awareness and training program", available at: http://csrc.nist.gov/publications/PubsSPs.html (accessed February 13, 2017).

Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol. 31 No. 5, pp. 673-680.

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

Peppard, J. and Ward, M. (2004), "Beyond strategic information systems: towards an IS capability", *Journal of Strategic Information Systems*, Vol. 13 No. 2, pp. 167-194.

Pfeffer, J. and Sutton, R.I. (1999), *The Knowing-Doing Gap: How Smart Companies Turn Knowledge Into Action*, Harvard Business Press, MA.

PMCF (2007), *Project Management Competency Framework*, 2nd ed., Project Management Institute, Newtown Square, available at: www.pmi.org/learning/library/project-manager-competency-development-framework-7376 (accessed February 13, 2017).

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Putri, F. and Hovav, A. (2014), "Employees' compliance with BYOD security policy: insights from reactance, organizational justice, and protection motivation theory", *Proceedings of the European Conference on Information Systems, Tel Aviv, June 9-11*.

Renck, R., Kahn, E.L. and Gardner, B.B. (1969), "Continuing education in R&D careers", DSF report, Prepared by the Social Research, Chicago, pp. 69-20.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, pp. 93-114.

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protected motivation", in Cacioppo, J.T. and Petty, R.E. (Eds), *Social Psychophysiology: A Sourcebook*, The Guilford Press, New York, NY, pp. 153-176.

Sandberg, J. (2010), "Understanding human competence at work: an interpretative approach", *Academy of Management Journal*, Vol. 43 No. 1, pp. 9-25.

Schippmann, J.S., Ash, R.A., Battista, M., Carr, L., Eyde, L.D., Hesketh, B., Kehoe, J., Pearlman, K., Prien, E.P. and Sanchez, J.I. (2000), "The practice of competency modeling", *Personnel Psychology*, Vol. 53 No. 3, pp. 703-740.

SHRM (2012), *SHRM Competency Model*, Society for Human Resource Management, VA, available at: www.shrm.org/learningandcareer/competency-model/pages/default.aspx (accessed February 13, 2017).

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *Management Information Systems Quarterly*, Vol. 34 No. 3, pp. 487-502.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: an empirical investigation", *IEEE Computer*, Vol. 43 No. 2, pp. 64-72.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Spencer, L.M. and Spencer, S.M. (1993), *Competence at Work: Models for Superior Performance*, Wiley, New York, NY.

Talib, Y.A. and Dhillon, G. (2015), "Employee ISP compliance intentions: an empirical test of empowerment", *Proceedings of the 2015 International Conference on Information Systems, Fort Worth, TX, December 12-16*.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs", *Computers & Security*, Vol. 52, July, pp. 128-141.

Vance, A. and Siponen, M. (2012), "IS security policy violations: a rational choice perspective", *Journal of Organizational and End User Computing*, Vol. 24 No. 1, pp. 21-41.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: insights from habit and protection motivation theory", *Information & Management*, Vol. 49 Nos 3-4, pp. 190-198.

Von Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R. and Cleven, A. (2009), "Reconstructing the giant: on the importance of rigour in documenting the literature search process", in Newell, S., Whitley, E., Pouloudi, N., Wareham, J. and Mathiassen, L. (Eds), *Proceedings of the 17th European Conference of Information Systems*, pp. 2206-2217.

Wall, J.D., Palvia, P. and Lowry, P.B. (2013), "Control-related motivations and information security policy compliance: the role of autonomy and efficacy", *Journal of Information Privacy and Security*, Vol. 9 No. 4, pp. 52-79.

Webster, J. and Watson, R. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, Vol. 26 No. 2, pp. xiii-xxiii.

Winterton, J. (2009), "Competences across Europe: highest common factor or lowest common denominator", *Journal of European Industrial Training*, Vol. 33 Nos 8/9, pp. 618-700.

Yang, X., Yue, W.T. and Sia, C.L. (2011), "A cross-cultural study of the effects of STEA programs and task characteristics on employees' behavior toward information system security policy compliance", *Proceedings of the 6th Mediterranean Conference on Information Systems, Limassol, September 3-5*.

Corresponding author
Aggeliki Tsohou can be contacted at: atsohou@ionio.gr

(The Appendix follows overleaf.)

Appendix

Table AI.
Results of IT-related competences and security competences as found in competence frameworks

Framework	Target groups	IT-related competences	Security-related competences
Project Management Competency Framework, Second Edition 2007	Project managers, managers of project managers, members of a project management office, managers responsible for establishing and developing project manager competence, project sponsors, educators teaching project management and other related subjects, trainers developing project management educational programs, consultants to the industry of project/program management, human resource managers, senior management, and individuals interested in project management	Element 2.5 Communication activities agreed – selects suitable tools and methods to communicate with identified stakeholders (p. 15) Element 6.3 Ensures quality of information – uses appropriate information sources (p. 27) Element 9.3 Uses appropriate project management tools and techniques – understands PM tools and techniques; selects appropriate tools and/or techniques; applies selected tools and/or techniques to project management (p. 33)	Element 8.2 Plans and manages for project success in an organized manner – insists on compliance with processes, procedures, and policies (p. 31)
APM Competence Framework, Association for Project Management, Second Edition 2015	Organizations and individuals engaged in project activities regardless of their size, sector or geographic location. Training providers for understanding the training needs of project professionals	Procurement competences – knows how to determine the type, quality and quantity of resources required to meet the objectives of change initiatives (K1, p. 9) Solutions development – knows tools and techniques to identify, evaluate and select alternative possible delivery options (K1, p. 12) and knows tools and techniques used for modeling, prototyping and testing (K2, p. 12) Schedule management – knows the use of scheduling tools and methods (K4, p. 13) Knows techniques to guide the choice, capture and analysis of relevant data (K5, p. 13) Resource management – knows techniques to guide the choice, capture and analysis of relevant data (K4, p. 14) Budgeting and cost control – knows tracking systems for actual	Contract management – complies with relevant organizational procedures and legal and ethical requirements when managing contracts (p. 10) Reviews – knows the legal, regulatory and organizational requirements for reviews (K1, p. 25)

(*continued*)

Framework	Target groups	IT-related competences	Security-related competences
		costs, accruals and committed costs (K4, p. 15) Quality management – knows inspection processes and analytical tools (K6, p. 17) Resource capacity planning – knows use of network diagrams to develop logical models; scenario analysis; and what if modeling (K2, p. 21), resource capacity planning tools and methods (K3, p. 21) and scheduling tools and methods (K4, p. 21) Stakeholders and communication management – knows the range of methods and media for communicating with stakeholders, and how to select the most appropriate methods (K. 3, p. 23) Capability development – knows the range of tools and techniques that can be used to assess organizational capability and individuals' skills and competence, and to identify their development needs (K1, p. 30)	
SHRM Competency Model, Society for Human Resource Management, 2012	Human resources professionals in different stages of their career, including early, mid, senior and executive levels	Competence 1: Human resource expertise – sub-competence: HR technology (p. 10) and relevant behaviors: maintains up-to-date knowledge of general HR practices, strategy, and technology (p. 10), uses relevant HR technology systems for administrative and service needs (p. 11) and recommends HR technology decisions (p. 12) Competency 3: consultation – behavior: gathers, and when appropriate, analyzes facts and data for business solutions (p. 17), uses appropriate analytic tools to provide other leaders input on strategic decisions (p. 18) Competency 5: communication – sub-competence: social technology and social media savvy (p. 22) and relevant behavior: provides clear, concise information to others in verbal, written, electronic, and other communication formats for public and organizational consumption (p. 22) and utilizes communication technology and social media (p. 22) Competency 8: critical evaluation – Behavior: analyzes data with a keen sense for what is useful and analyzes large quantities of information from research and practice (p. 32) Competency 9: business acumen – sub-competence: knowledge of	Competency 1: human resource expertise–behavior: remains current on relevant laws, legal rulings, and regulations (p. 10) Competency 4: leadership and navigation – behavior: understands the most effective and efficient way to accomplish tasks within the parameters of organizational hierarchy, processes, systems, and policies (p. 19) Competency 5: communication – behavior: communicates and implements policies on social media Competency 7: ethical

(*continued*)

Table AI.

Table AI.

Framework	Target groups	IT-related competences	Security-related competences
		technology (p. 35) and relevant behaviors: leverages technology to solve business problems (p. 35), implements HR and business technology plans to solve business problems and needs (p. 36)	practice – behavior: creates processes to ensure confidentiality and privacy of employee information and company data (p. 29)
HRPA competency model, Human Resources Professionals Association 2014	Provides credential information for the certification of human resources professionals. Targets trainers using the model for establishing education requirements, for examination development, and for career planning. Targets human resources professionals and any employers and employee	Enabling competency: technological savvy – making use of various technologies to best advantage, seeing the possibilities in emerging technologies and managing the implementation of new technologies (p. 26) C001: maintain awareness of broad economic, societal, technological, political, global, and demographic trends (p. 28) C002: identify HR opportunities and risks inherent in changes in economic, societal, technological, political, and demographic forces (p. 27) C049: evaluate the applicability of new concepts and technology to the practice of HR within the organization (p. 52) C208: evaluate alternative tools for the maintenance of HR information (p. 132) C209: use effective and efficient HR information retention tools (p. 132)	C183: establish health, safety, and wellness policies, procedures, roles, and responsibilities for leaders and employees that meet organizational compliance standards (p. 120)
CGMA (2014), Chartered Global Management Accountant, Chartered Institute of Management Accountants and the Association of International Certified Professional Accountants	Management accountants and their employers in order to understand the knowledge requirements and assess the skills needed for both current and desired roles	Corporate finance and treasury management: identify and exploit technology and market trends to define future best practice in cash management solutions to meet business needs (p. 18) Accounting information systems: several competencies per professional level, indicatively Obtain working knowledge of the organization's information systems environment (hardware, software and networks), Monitor the applications and effectiveness of the organization's information systems, develop and communicate strategic vision regarding the finance systems and supporting technology (p. 28) Demonstrate understanding of the accounting systems and their functionality (p. 29)	Accounting information systems: technology developments and IT solutions – analyze external IT developments for data integrity and access control management (p. 30)

(*continued*)

Framework	Target groups	IT-related competences	Security-related competences
		Understand applicability of new and improved IT developments and solutions (p. 30) Market and regulatory environment: devise information reporting tools to aid the understanding of regulatory stakeholders (p. 39) Business relations: understand the tools and systems for contract creation and compilation, change control and variations and maintain appropriate contract documentation (p. 41) Project management: develop simple project plans including business case, contingencies, critical paths and apply project management tools and techniques (p. 42)	
IFMA (2016), International Facility Management Association	Facility managers and organizations aiming to assure professional excellence, establish standards for global professional practice, and influence the future direction of the profession	Competency area communication: select the situation-appropriate media and techniques for communicating with stakeholders (p. 2) Competency area quality: collect, verify, analyze and report facility management data from various sources (p. 7) and collect and verify, analyze and report internal facility management data (p. 7) Competency area technology: monitor and evaluate technology trends and innovation, conduct assessments and/or collaborate on facility management technology needs analysis, align facility management technology with organizational information technology, assess the application of technology within facility operations and evaluate, implement and operate integrated workplace management systems (IWMS – combining CAFM, CMMS and BAS) (p. 8)	Competency area emergency preparedness and business continuity: secure technology systems and services (p. 2) and develop a business continuity plan (p. 2) Competency area human factors: provide security that meets the facilities' needs (physical, site security, access control, information) (p. 4) Competency area quality: audit and document compliance with codes, regulations, policies and standards (p. 7) and ensure compliance with codes, regulations, policies and standards (p. 7)
IAF (2015), International Association of Facilitators	Includes competencies that form the basic set of skills, knowledge, and behaviors that facilitators must have in	Competence area – guide group to appropriate and useful outcomes: identify information the group needs, and draw out data and insight from the group (p. 3)	

(*continued*)

Table AI.

Table AI.

Framework	Target groups	IT-related competences	Security-related competences
	order to be successful facilitating in a wide variety of environments		
IAAP (2016), International Association for Administrative Professionals	Targets office management and business administrative professionals. It is aligned with the Certified Administrative Professional Certification running by the IAAP	Domain organizational communication: explain the importance of professional networking and what can be accomplished through social networks (p. 2) Domain business writing and document production: know which software applications are appropriate for the production of common business documents (p. 4) and knowledge of and proficiency with spreadsheet creation, including simple formulas and data manipulation (p. 4), and know which software is appropriate for office design and publishing in addition to their features and functions (p. 4), demonstrate a familiarity and proficiency with online tools for web publishing (p. 4), demonstrate a basic knowledge of and proficiency with software applications needed to create, format, and insert charts, tables and graphs into business documents and presentations (p. 4) Domain technology and information distribution: demonstrate knowledge and proficiency of different e-mail interface types (p. 5), identify and describe the process and techniques of gathering, compiling, and analyzing data (p. 5), basic knowledge and proficiency in installation, maintenance, and troubleshooting both equipment and software problems (p. 5) basic knowledge and proficiency in the use of the internet as a way of communicating with others inside and outside of the organization (p. 5), identify and describe common ways of storing and transferring data and the types of media appropriate for each Domain office and records management: know available software, systems, and services for electronic filing, including characteristics and costs (p. 6)	Domain technology and information distribution: identify and describe copyright laws, regulations regarding intellectual property, and ways to maintain confidentiality when distributing information (p. 5), Explain what security procedures are involved in maintaining, backing up, and storing information (p. 5) Domain office and records management: identify and describe the appropriate security for both electronic and manual files (identify the key laws regarding record storage and confidentiality and Identify both the strengths and weaknesses of types of record and file security) (p. 6) Domain human resources: identify the procedures for maintaining confidentially of employee records (p. 8)