11-28-2018

Designing for Knowledge Based Cyber-Security – Episode 1: What Should We Teach?

Peter Heinrich
ZHAW School of Management and Law, peter.heinrich@zhaw.ch

Axel Uhl
ZHAW School of Management and Law, axel.uhl@zhaw.ch

Monika Josi
COCUS Schweiz AG, monika.josi@axas.ch

DESIGNING FOR KNOWLEDGE BASED CYBER-SECURITY – EPISODE 1: WHAT SHOULD WE TEACH?

Research paper

"It is a mistake to think you can solve any major problems just with potatoes."
- Douglas Adams

Heinrich, Peter, ZHAW School of Management and Law, peter.heinrich@zhaw.ch

Uhl, Axel, ZHAW School of Management and Law, axel.uhl@zhaw.ch

Josi, Monika, COCUS Schweiz AG, monika.josi@cocus.ch

Abstract

Cybercrime proliferates and cyber-security seems evermore challenging. Literature offers large support that cyber-security is rather of behavioral than of pure technical matter. While prior research has focused on explaining organizational and individual (mis)behavior and agreed on the crucial role of cyber-security education programs, less is known on the question of what to teach in order to change behavior. With an exhaustive literature review, this article helps to build a foundation for developing training based interventions, grounded on strong behavioral models, taking a knowledge management view to foster behavioral change by supplying relevant knowledge entities. Embedded in a stream of design science research (DSR) activities this article reports on DSR's first two phases, problem description and definition of solution objectives. This article ends with a set of design requirements to a cyber-security training environment in terms of content and learning approach grounded on the results of the literature review.

Keywords: Cyber-Security Training, Knowledge, Protective Behavior

1 Introduction

We should not be seeing a large-scale crisis in cyber-security. Economically, successful attacks and breaches are a disaster, both financially and/or in terms of reputation. Although the topic is strongly discussed both in scientific and public media, companies invest vast amounts into cyber-security, and governmental regulations seek to enforce stringent policies and procedures, the field looks something like Don Quixote's attacks on windmills. According to a 2016 practitioner study (CyberEdge Group, 2016) with n = 943 companies across the world, more than 75% of them had been successfully attacked at least once during a 12-month timespan. Further, according to Intel Security, 82% of companies have skills shortages and 70% even attribute a direct loss to this shortcoming (McAffee, Part of Intel Security, 2016).

Thus, one could generally argue that, since companies are well aware of the dangers, they would change their behaviors and manage their security better. This would rule out the viewpoint of the well-known article *Unskilled and Unaware of It* (Kruger and Dunning, 1999), in which the authors argue that under a certain competence level, self-assessment of skills and competence fails and knowledge gaps remaining therefore go undetected. On the one hand, given the vast amount of media coverage and self-reported skills shortages, this seems implausible. But on the other hand, 38% of the aforementioned CyberEdge Group study's participants still believe it is unlikely (!) that they will be hacked again in the next 12 months. While individuals are swamped by reports about incidents in the public media and specialized publications, knowledge is accessible via the Internet in mass quantity, and since financial motivation is high, we should expect to see changes in behaviors. However, this does not seem to be the case.

Generally, there are many possible ways to approach this problem, and much research effort has gone into the development of technical interventions. However, we focus on the behavioral perspective. As largely agreed in literature (e.g. C. C. Chen, Shaw and Yang, 2006; Karjalainen and Siponen, 2011; Tsohou, Karyda, Kokolakis and Kiountouzis, 2015) education and awareness training are important approaches to raise cyber-security. However, surprisingly little is known on the question of what to teach exactly and for what specific reason. Thus, our main design goal is:

Design goal (DG): *To raise cyber-security by identifying, assessing, and training in the required skills and knowledge.*

In the spirit of design science research, we describe the first two phases of the design science research process (Peffers, Tuunanen, Rothenberger and Chatterjee, 2007): (1) the identification and description of a design problem and (2) the envisioned solution objective. We first analyze the existing body of knowledge by performing a systematic and exhaustive literature review on the topic. Based on the identified and relevant articles, we derive a set of generic requirements to a solution that seeks to raise cyber-security via specific provision of knowledge. Thus, we seek to answers to the following research questions (RQs):

RQ1: *What behavioral concepts and theories describe the adoption of protective behaviors and can thus inform the design of a knowledge management system and learning environment?*

RQ2: *What challenges exist that hinder successful knowledge transfer?*

With these results, researchers can engage in designing *abstract* and *specific solutions* (cf. Lee, Pries-Heje and Baskerville, 2011), validating and extending these design objectives, identifying design principles, and ultimately framing the gained design knowledge in a *design theory* (cf. Gregor and Jones, 2007).

1.1 Background

We now turn to a basic definition of cyber-security: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen, Diakun-Thibault and Purse, 2014, p. 13). Thus, to enable cyber-security, the actors must be willing and capable to manage resources, create processes, and instantiate structures. In practice, this seems to be a very difficult endeavor. First, the topic is complex; second, the threats and technological means are constantly and rapidly changing.

In the past, cyber-security was much easier, and a strategy to prevent being breached by securing the perimeter was sufficient. However, this is no longer plausible. With the rise of *Software as a Service* (SaaS), *bring your own device* (byod) and collaborative work using cloud infrastructures, there is no longer a clear distinction between inside and outside. Further, the acceptance of an imperfect world demands information security strategies that focus on detection and response instead of relying solely on protection and prevention (Pompon, 2016). In fact, the literature offers many different approaches, in both in temporal and functional dimensions. The temporal dimension divides the strategies into a *prevention paradigm* and a *response paradigm* (Baskerville, Spagnoletti and Kim, 2014). These dimensions differ greatly in their underlying assumptions, principles, and logical structures. While the *prevention paradigm* relies on stable, measurable threats and safeguarding against threats as necessary and sufficient, the *response paradigm* offers a much more open and dynamic view on threats, acknowledges their transience and unpredictability, and sees safeguarding as necessary but insufficient (Baskerville et al., 2014). The *assume breach* strategy overlaps with the response paradigm. Functionally, the response paradigm can be dissected further: besides prevention and response, the literature offers *deterrence*, *surveillance*, *detection*, *deception*, *perimeter defense*, *compartmentalization*, and *layering* as complementary strategic opportunities to combat cybercrime (Ahmad, Maynard and Park, 2014). *Deterrence* seeks to keep people from illicit behaviors through fear of disciplinary action (D'arcy and Herath, 2011; Ahmad et al., 2014) and is a strategy focused on inside threats. *Surveillance* seeks to increase situational awareness by continuously monitoring the environment (Ahmad et al., 2014), but can also influence an individual's behavior if they knows that they are being monitored (Boss et al., 2009). *Detection* may sound like an extraordinary trivial strategic approach, but considering that organizations need no less than 99 (!) days on average to detect a breach ("M-Trends 2017 Cyber Security Trends," 2017) there is still much potential for optimization. *Deception* assumes that an attacker has already violated the system's boundaries and aims at distract them so that they waste time and resources, giving the organization more time to respond (Ahmad et al., 2014). *Perimeter defense*, *compartmentalization*, or *layering* fall outside the scope of this article, as these are common, well-known, widely applied, preventative, and often purely technical or organizational approaches.

Although the technical interventions are well understood and widely applied, "true security" has remained unattainable. The literature acknowledges that people are often the weak link and that their behavior is susceptible to malicious practices (e.g. Boss et al., 2009; Parsons et al., 2014; Safa et al., 2015; Rocha Flores and Ekstedt, 2016; Öğütçü, Testik and Chouseinoglou, 2016). Thus, we assume that the problem still persists, even if technical issues could eventually be solved. We will now look at behavioral effects on an individual and an organizational scale.

2 Method

We applied the *design science research (DSR) in information systems* research paradigm (A. Hevner, March, Park and Ram, 2004). In contrast to natural or behavioral scientific paradigms, design science research asks how future artifacts can be designed in order to obtain specific goals that are valuable to someone. DSR activities span three cycles: (1) relevance cycle, (2) build/evaluate cycle, and (3) rigor cycle (A. R. Hevner, 2007). While the relevance cycle retrieves the requirements from the field, the rigor cycle grounds problems and solutions to the available body of scientific knowledge. According to Hevner's (2004) guidelines, DSR must: (1) produce an artifact, (2) be relevant and solve important problems, (3) be evaluated rigorously, (4) provide clear research contributions, (5) apply rigorous methods, (6) be carried out as a search process, and (7) be communicated. Although this article is the first publication in a stream of research activities, it can already fulfill most but not all guidelines: (1) This article contributes a consolidated design research model and a set of design objectives as its core artifact. In future project stages, other artifacts such as system implementations that build on this model will follow. (2) We demonstrate the relevance of insufficient cyber-security by highlighting the massive financial losses and large body of publications on the subject. (3) While an empirical grounding of the proposed design objectives is still lacking, we ground our model on the current body of literature, applying explanatory, value, and conceptual grounding strategies (cf. Goldkuhl, 2004). (4) Further, we contribute a consolidated model as the basis for further design research activities and explicitly call for research in this area. (5) The steps we performed followed rigorous processes, and the systematic literature review (see below) is presented with the intent of transparency. (6) Overall, with this article, we build the basis for the upcoming (design) search process. In addition, we partially fulfill guideline (7): While this publication just describes the first two phases, many further publications need to follow to exhaustively describe the search and evaluation process and carry all created knowledge back into the scientific community.

Besides these seven guidelines, DSR projects commonly follow a cyclic structure of the following six steps (Peffers et al., 2007): (a) problem identification, (b) a solution's objectives, (c) design and development, (d) demonstration, (e) evaluation, and (f) communication. Following this process model, this article spans activities (a) and (b) and communicates (f) these results.

As the first step in the rigor cycle, we did a systematic and exhaustive literature review following the suggestions of Webster et al. (2002) and Vom Brocke et al. (2009) concerning the categorization of the results and search strategy. Since cyber-security is inherently interdisciplinary, we opted for an exhaustive database search approach. The documentation of the precise search process, databases used, and keywords applied follows.

3 Grounding the problem: A Literature Review on Knowledge Based Cyber-Security

We selected seven very common IS-related databases for our literature search (see Table 1). Also, we included Google Scholar as meta-search engine so as to further minimize the risk of missing relevant publications. The search queries in conjunctive normal form (CNF) contained two clauses: one clause selected the cyber-security domain in different words (cybersecurity, cyber-security, or cyber security); the second clause selected the knowledge aspect, represented by certain terms (knowledge, literacy, skills, or awareness). We found that all selected databases (except Google Scholar) directly accepted queries in CNF. The query execution included searches of titles, keywords, and abstracts. The final query was:

(cybersecurity OR cyber-security OR cyber security) AND (literacy OR knowledge OR skills OR awareness)

In a first step, we selected relevant publications based on their titles and abstracts. Table 1 provides an overview of the initial search results and the first filter operation based on the title and abstract (when unclear).

After removing duplicates, books, abstracts only, and panel discussions, the set was reduced to 347 articles. For these articles, we retrieved the full text version. However, despite our efforts to configure the databases to return only scientific, peer-reviewed journals, the result set still contained 65 items of practical reports and guidelines, not meeting standards of scientific discourse (i.e. containing hardly any or no references). Further, we only included full-length articles of 9 pages or more (thus, we removed another 149 articles).

Library	Number of initial results	Results included based on title / abstract filtering
ACM Digital Library	228	63
AIS Electronic Library	100	18
EBSCOhost	142	33
IEEE Xplore Digital Library	536	56
Science Direct	1,625	106
WebOfScience	160	47
Proquest	920	74
Google Scholar	125	57

Table 1. Search Results by Databases

This left 133 articles for further analysis. From this set, we identified the actively discussed articles, since these form part of the scientific discourse. Google Scholar provided the citation count for each of these 133 articles. Based on the publication year, we set the inclusion criteria according to the following formula:

$$min\_cites = (2017 - Publication\_Year) * 5 + 1$$

Of the articles, 40 met this inclusion criterion – being cited at least once if published in 2017, at least six times if published in 2016, and at least 13 times if published in 2015, and so on. Additional 4 articles did not cover the subject or were of pure technical matter. The final set therefore consists of 36 articles (see Table 3). Table 2 provides an overview of the journals that contained more than one article.

Journal title	Number of articles
Computers & Security	14
European Journal of Information Systems	4
Computers in Human Behavior	3
Information & Management	2
Journal of the Association for Information Systems	2

Table 2. Identified Key Journals

Of the articles, 22 described individual behaviors and 14 incorporated a group-wide/organization-wide view on cyber-security; 30 focused on behavior or state-of-the-art implementations, only three articles provided design guidelines or frameworks. One of these three articles is a meta-study that identified no less than 32 approaches described in the literature, all of which address particular pedagogical requirements (context, content, method, and evaluation) (Karjalainen and Siponen, 2011). Karjalainen and Siponen (2011) called for research to (1) a validation of training perspective, (2) critical-level pedagogical principles, and (3) an experiential and collaborative perspective. We responded to this call – this article seeks to provide required theoretical underpinning by identifying the behavioral theories used to explain individuals' and groups' engagement to security enhancing behaviors. Table 3 provides an overview of the constructs, theories, and models used in the identified papers.

				Theories / Models from Problem Space															Biases		Constructs from Solution Space							
	Group / Organization	Individual	Design / Framework	PMT	TPB / TRA	GDT	KAB	TTAT	Control Theory	Social Bond Theory	Involvement Theory	ANT	TAM/UTAUT	Structuration Theory	Real option Theory	Contextualism	Socio-Ecological Systems	Rhetoric Framing	Cognitive	Cultural	Awareness	Attack Detection	Habitats	Security Strategies	Transf. Leadership	Knowledge Sharing / Learning	Managerial practices / Culture	Learning Theories
(Franke and Brynielsson, 2014)	x	x																			x							
(Soomro, Shah and Ahmed, 2016)	x																				x						x	
(Flores, Antonsen and Ekstedt, 2014)	x																									x	x	
(Sikula, Mancillas, Linkov and Mcdonagh, 2015)	x																x											
(Boss et al., 2009)	x	x							x																			
(Tsohou, Karyda, Kokolakis, et al., 2015)	x											x		x		x												
(Quigley, Burns and Stallard, 2015)	x																	x										
(Posey, Roberts, Lowry and Hightower, 2014)	x	x		x																								
(Baskerville et al., 2014)	x																							x				
(Keller et al., 2005)	x																											
(Atoum, Otoom and Ali, 2017)	x		x																									
(Gordon, Loeb, Lucyshyn and Zhou, 2015)	x														x											x		
(Ahmad et al., 2014)	x																							x				
(Usman and Shah, 2013)	x																											
(Imgraben, Engelbrecht and Choo, 2014)		x																			x				x			
(Jeske and van Schaik, 2017)		x										x									x							
(Öğütçü et al., 2016)		x																			x							
(Parsons et al., 2017)		x																			x							
(Parsons et al., 2014)		x					x														x							
(Safa and Von Solms, 2016)		x		x	x																x							
(C. C. Chen et al., 2006)		x	x																		x					x		
(Zafar, Randolph and Martin, 2017)		x		x									x										x					
(Pfleeger and Caputo, 2012)		x			x														x									
(Rocha Flores and Ekstedt, 2016)		x			x																x				x		x	
(Safa et al., 2015)		x		x	x																							
(Sohrabi Safa, Von Solms and Furnell, 2016)		x								x	x															x	x	
(Tsohou, Karyda and Kokolakis, 2015)		x																	x	x	x							
(Ben-Asher and Gonzalez, 2015)		x																				x						
(Junger, Montoya and Overink, 2017)		x																	x									
(D'arcy and Herath, 2011)		x				x																						
(Herath and Rao, 2009)		x		x	x	x																						
(Woon, Tan and Low, 2005)		x		x																								
(Purkait, 2012)		x																										
(Dinev and Hu, 2007)		x			x								x															
(Karjalainen and Siponen, 2011)		x	x																									x
(Y. Chen and Zahedi, 2016)		x			x			x																				

Table 3. Theories and constructs used in the identified literature.

In the following sections, we explain the key theories in cyber-security, such as the *theory of planned behavior* (TPB) (Dinev and Hu, 2007; Herath and Rao, 2009; Safa et al., 2015; Rocha Flores and Ekstedt, 2016; Safa and Von Solms, 2016), *protection motivation theory* (PMT) (Woon et al., 2005; Herath and Rao, 2009; Posey et al., 2014; Safa et al., 2015; Safa and Von Solms, 2016; Zafar et al., 2017), *general deterrence theory* (GDT) (Herath and Rao, 2009; D'arcy and Herath, 2011), the *technology acceptance model* (TAM) (Dinev and Hu, 2007; Tsohou, Karyda, Kokolakis, et al., 2015), the concept of *threat and situation awareness (awareness)* (C. C. Chen et al., 2006; Franke and Brynielsson, 2014; Imgraben et al., 2014; Parsons et al., 2014; Safa and Von Solms, 2016; Soomro et al., 2016; Öğütçü et al., 2016; Parsons et al., 2017; Jeske and van Schaik, 2017), and cognitive as well as cultural behavioral biases that hinder adoption (Pfleeger and Caputo, 2012; Tsohou, Karyda and Kokolakis, 2015; Junger et al., 2017).

3.1 The Theory of Planned Behavior (TPB)

The theory of planned behavior (TPB) is a more general behavioral theory that is not specific to threat protection. Originally developed by Ajzen (1985, 1991), PTB described the mechanisms of goal-oriented behavior. Its three primary independent variables are attitude, subjective norms, and perceived behavioral control. In this theory, the attitude is the sum of two parts: (1) the (obvious) attitude towards goal attendance and (2) the attitude towards failure. Both variables are weighted with the perceived probability. However, Ajzen explicitly notes that these variables can only explain a subject's intention to perform a specific behavior. The de facto execution of a behavior is subject to (a) the intention and (b) the abilities concerning skills and information (Ajzen, 1985). Safa et al. (2015) applied TPB and PMT together to explain what they called *security-conscious care behavior*. Thus, this model, applied in the cyber-security context, can explain why individuals engage in protective activities. According to this theoretical model, individuals may only engage in protective behavior if they can attain a certain individual goal without investing a prohibitive amount of effort. However, in contrast to the original model, Safa et al. (2015) could not show a significant correlation between the perceived behavioral control and the behavior. This is supported by TPB, since "This correlation will tend to be strong only when perceived control corresponds reasonably well to actual control" (Ajzen, 1985, p. 34).

3.2 Protection Motivation Theory (PMT)

At the level of a single individual, protection motivation theory (PMT) seems to be the most commonly used model. Originally developed and refined by Maddux and Rogers (1983), PMT uses the constructs of threat appraisal (TA) and coping appraisal (CA) to generally explain engagement in protective behavior. The original research used the scenario of giving up smoking as an example of a protective behavior and a high-consequence threat. They found that a high threat probability and an effective coping strategy had positive effects on the intention to protect oneself (Maddux and Rogers, 1983). Woon et al. (2005) adapted the model to IS security – in particular to wireless network security. In line with Maddux and Rogers, perceived vulnerability to threats and perceived threat severity both add to TA, while perceived response efficacy and perceived self-efficacy add to CA. In this example, Woon et al. (2005) could demonstrate that owners of an unprotected wireless network were highly troubled by security concerns, but were also unable to act. They explained this controversy by arguing that although there was a high threat appraisal in this case, the skills lack resulted in low self-efficacy and low response efficacy; thus, the subjects were unmotivated to act. Both appraisals are tradeoffs between costs, fears, and benefits. While, as demonstrated, the costs of the response weakens the coping appraisal (Woon et al., 2005), rewards for maladaptation (i.e. fooling oneself about severity or vulnerability) also weakens the threat appraisal (Posey et al., 2014).

3.3 General Deterrence Theory (GDT)

While protection motivation theory focuses on intrinsic motivation, deterrence theory focuses on extrinsic motivation. Its main goal is to prevent criminal activity by means of fear. Originally developed in the mid-1970s (Gibbs, 1975), GTD explains desistance from criminal activity as a tradeoff between reward and fear for punishment, expressed by perceived sanction severity and probability. The word *general* relates to its focus on the general public, which has to date not engaged in criminal activity, while specific deterrence theory focuses on individuals who have already committed crime (Stafford and Warr, 1993). The reviewed cyber-security literature only focused on general deterrence theory. In line with early deterrence research, deterrence's effectiveness in the cyber-security domain strongly depends on an individual's characteristics, such as *self-control*, *morality*, or *virtual status (i.e. working* *remotely)* (D'arcy and Herath, 2011). D'arcy and Herath (2011) argue that these contingency variables moderate deterrence's effectiveness and that *computer self-efficacy* might even have a negative effect on deterrence as it leads to the belief that one is too clever to get caught. At first glance, this seems to contradict PMT, since self-efficacy relates positively to protective behavioral intention (see sections above). However, this is unsurprising, since the theories differ concerning an individual's intention. While GDT assumes that any individual could potentially become involved in criminal activities if they are not deterred, they may use this knowledge to bypass punishment, PMT argues that an individuals can use their skills to protect themselves from external criminal activities (or other actions with negative effects), raising coping appraisal. That said, self-efficacy's double-sidedness may well be present in all crime-related topics; this is also a recurring topic in higher computer science education concerning whether or not to teach specific hacking skills (Logan and Clarkson, 2005).

3.4 The Technology Acceptance Model (TAM)

Preventative behavior sometimes includes the use of certain protective technologies. In the case of cyber-security, this could be a virus scanner or a password manager. The *technology acceptance model* seeks to explain a user's intention to use a given technology, given its perceived usefulness and ease-of-use. Originally developed by Davis et al. (1989), TAM sets out to explain the use of positive technologies (Dinev and Hu, 2007) (i.e. technologies that provide value to some individual). In contrast, a virus scanner would be a preventative technology (Dinev and Hu, 2007), i.e. its only value is to prevent bad things from happening. Interestingly, other dimensions seem to be important to explain the use of this kind of technology, rather than perceived usefulness and perceived ease-of-use. Its main purpose (besides potentially preventing something) is to calm individuals who fear sanctions if the technology is not used (Dinev and Hu, 2007). This is especially true in the case of virus scanners: their effectiveness are an open question (Thamsirarak, Seethongchuen and Ratanaworabhan, 2015); while the use of virus scanners is laypersons' top security preventative measure, security experts have very different topics on their high-priority list, starting with a patched and updated overall system installation (Ion, Reeder and Consolvo, 2015).

3.5 Awareness

The concept of awareness has a dual purpose in cyber-security. One role is 'classical' awareness in terms of *situation awareness* (cf. Endsley, 1995). This includes the ability to perceive and react properly to external security-related events that could be "any kind of suspicious/interesting activity taking place in cyberspace" (Franke and Brynielsson, 2014, p. 20). Awareness' other role describes an individual's awareness of a particular feature in their environment. This could be knowledge of the existence of a specific, preventative *technology* (Dinev and Hu, 2007), general knowledge of existing *threats* (Parsons et al., 2014), or even knowing that one's actions are *monitored* (Boss et al., 2009).

While the underlying causal logic of the second role seems more trivial along the lines that one cannot consider things one does not know, the causal relationships of situational awareness are more complex. Endsley (1995) states that an individual's decisions are subject to the cognitive processes of *perception of events*, *understanding of the current situation*, and the *projection of the situation onto the future.* However, Endsley's (1995) model also describes individual attributes' influences on decision-making processes such as personal experience, abilities, training, or personal expectations and objectives. Thus, these causal relationships seem compatible with PMT and TPB.

3.6 General Biases

While the presented theories can to an extent explain users' observable behaviors, they also reveal that security-related behavior strongly depends on an individual's perception of the world (i.e. individuals' perceptions of threats, their own capabilities, the normative context, etc.). Further, the literature describes a series of biases that impact on the 'rational' behavior proclaimed by some of these theories.

Consider some potential biases listed by Pfleeger and Caputo (2012): *Identifiable victim effect*: Individuals may pay less attention to abstract threats that are disconnected from their personal context. *Bystander effect*: Even if individuals properly note a threat, they still may not engage in countermeasures based on the belief that someone else will take care of it (i.e. the system administrators). *Status quo bias*: People tend to keep their practices and need strong motivation for behavioral change. *Optimism bias*: Individuals tend to perceive risks as less likely, although they know the dangers.

3.7 Organizational Biases

Because individuals are the biggest threat to cyber-security, the topic is also relevant at the organizational level. Top managers' involvement is a necessity for any cyber-security initiative to produce meaningful results (Barton, Tejay, Lane and Terrell, 2016). However, managers are susceptible to behavioral biases as well. For instance, managers' participation in information system security appears to depend only on their belief system, which in turn seems only depend on what the competitors do – i.e. merely mimicking their behavior (Barton et al., 2016). This observation further substantiates the importance of inter-organizational and intra-organizational knowledge-sharing. A current study even posits that information-sharing can prevent under-investment in information security (Gordon et al., 2015). Nonetheless, sharing information only between similar firms also raises the dangers of cyclical dependencies, which hinder real innovations. Further, sharing cyber-security-related information can also be crucial in terms of legal constraints or can negatively impact on a company's competitiveness (Gordon et al., 2015). Thus, establishing information-sharing is a delicate process that is influenced by the organizational structure and how the coordination process in the organization aligns business risks and security demands to appropriate controls (Flores et al., 2014).

3.8 Defining an Abstract Problem

Summing up the individual factors, a pattern seems to emerge: If threats cannot be repelled automatically/technically, individuals (or groups of them) need specific knowledge, attitudes, and skills to detect a problem and create a coping strategy. However, malicious incentives, individual properties, and individual perceptions can hinder the execution of required actions, even if these were known to the individuals. Thus, the presence of appropriate knowledge and skills are necessary but not sufficient to effectively trigger action. We can therefore conclude that not only functional knowledge is required, but also knowledge that can change attitudes and perceptions. A near-perfect example could be observed when researching individuals' susceptibility to phishing, where participants were explicitly primed and informed on the dangers of such attacks, but later happily disclosed random personal information (e.g. parts of their bank account number) to the 'unknown' researchers (Junger et al., 2017). Thus, the effect of knowledge on security problems alone is insufficient to induce a change in behavior.

Interestingly, in the literature review, many papers modeled individuals' behavior and explained why people make bogus information security decisions. However, there were few papers on how to change these behaviors. At least for management activities, there was one meta-study (Soomro et al., 2016) that strengthens management activities' necessary role for implementing cyber-security.

Thus, we define the problem of cyber-security implementation as the challenge to the organization to transform its employees' individual value systems, perceptions, awareness, skills and knowledge levels towards security-enhancing practices. Given the large number of successful cyber-attacks and the high associated financial losses, we consider these dimensions currently to be suboptimal at best. The specific challenges here are the circumvention of obstructive individual biases as well as organizational behavioral patterns that hinder the comprehensive implementation of protection. We will now seek possible design approaches and will define a set of objectives that a system should meet in order to have a measurable positive effect on cyber-security.

4 Deriving Objectives of a Design Solution

After reviewing the behavioral models and possible behavioral biases and obstacles, we now turn to the exploration of the solutions space, to identify realistic objectives that a solution design should accomplish. As noted, there may be many different approaches to this design problem. We opted for a solution that focuses on knowledge management, providing and transferring specific knowledge and skills to individuals and groups with the aim of altering their current attitudes, perceptions, self-efficacy, and skills to effectively circumvent behavioral obstacles. Figure 1 provides an overview of the consolidated behavioral design model. The consolidated behavioral model aggregate the many different theoretical views, all of which proclaim effects on behavioral intention. Without a necessary knowledge level (capabilities in general), the intended behavior cannot be executed. Woon et al. (2005) showed this for home wireless users who felt in danger owing to their unprotected (unencrypted) wireless network, but who did not have the necessary skills to change the situation. A direct path from information to behavioral intention derives only from *social cognitive theory (SCT)*, where the authors argue that prevention campaigns (health-care setting) transmitted via public media can partially influence behavioral intention also directly (Bandura, 2004). However, knowledge provision embedded in a social setting has much more potential to induce a behavioral change (Bandura, 2004).

Given the general availability of information and the still low cyber-security levels, we can safely conclude that access to knowledge alone is insufficient. The design idea, that we want to advocate in this paper is targeting the educational effort to the identified theoretical constructs, that could be susceptible to knowledge transfer and learning (highlighted elements in Figure 1). Let us now formulate design objectives and associated challenges based on the discussion of the identified theoretical contributions.

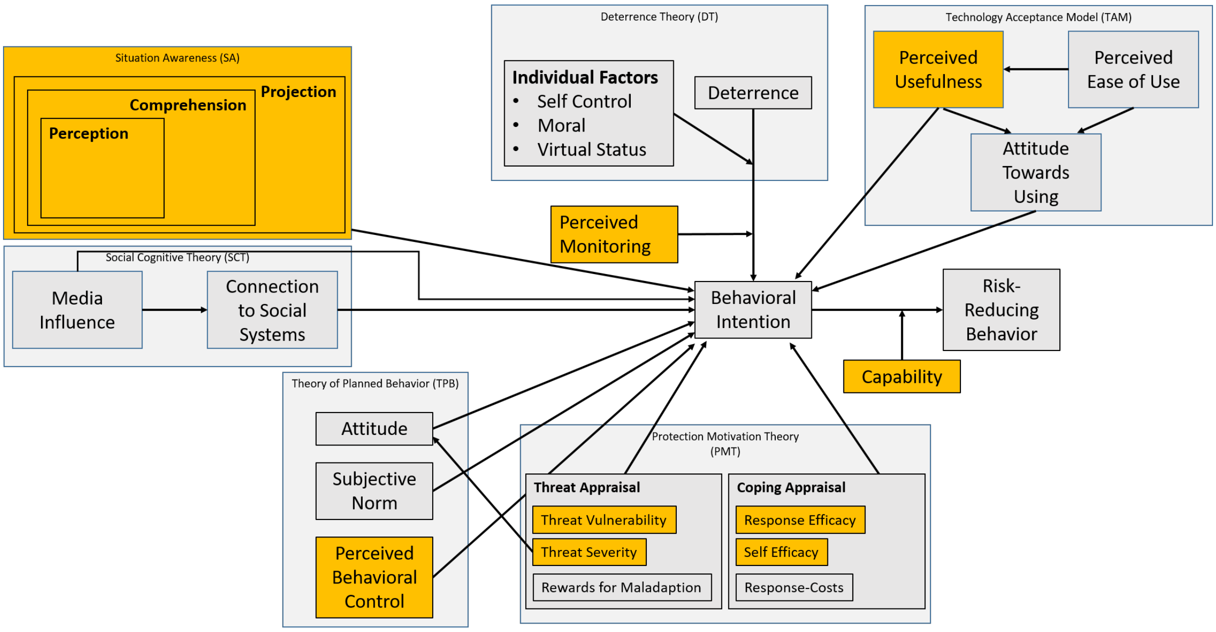

Figure 1: Consolidated Behavioral Design Model (model extended from Lebek et al., 2014) – highlighted elements are likely sensitive to learning and knowledge transfer.

First, instead of just providing generic cyber-security information to employees and decision makers, the learning environment should target the independent variables of the theoretical models that explain or predict the intention to engage in predictive behavior. Thus, learning efforts should specifically focus on *threat appraisal*, *coping appraisal*, *perceived behavioral control*, *perceived usefulness* (of protective technology), the *monitoring* actions taken, elements of *situation awareness*, and/or most importantly on the *capabilities* to transform intention into action. For these constructs, we argue that a transfer of appropriate knowledge would also change behavior. Thus:

Objective 0: A*ll learning efforts should explicitly target one or more elements of the behavioral design model that are susceptible to a change in knowledge levels.*

Design challenge 0: *Selecting the theoretical focus for a learning topic to maximize the impact on the behavioral intention.*

Generally, knowledge's role is diversely discussed in the literature: On the one hand, according to Safa et al. (2015), knowledge has a positive influence on behavior, such as "Keeping employees updated in terms of information security and increasing their knowledge in this domain have a significant effect on their behavior" (Safa et al., 2015, p. 76). On the other hand, medical research could show that self-efficacy moderates (Rimal, 2000) or at least mediates (Bandura, 2004) knowledge's effect on behavior. This also seems applicable in cyber-security, since information security research has shown that self-efficacy significantly correlates with security-enhancing behavior (Woon et al., 2005). Thus:

Objective 1: *Explicitly raise self-efficacy and keep knowledge buildup congruent with the computer self-efficacy level.*

Design challenge 1: *Continuously monitor individuals' self-efficacy and match educational content to these levels.*

Further, increased self-efficacy also has other positive effects. One approach is to engage people in self-monitoring cycles. In preventative health-care settings (e.g. reducing dietary fat intake), participants were far superior when they could operate in a self-monitoring setting, compared to a purely educative setting (Bandura, 2004). In cyber-security, this may be much more demanding, since protective behavior is not a simple one-dimensional measure, compared to weight or cholesterol level.

Objective 2: *Enable self-monitoring cycles and self-guided learning for all knowledge intended to cause behavioral changes.*

Design challenge 2: Development of s*elf-assessment capabilities for individuals to continuously measure their progress on behavioral change and set manageable goals for identified learning topics.*

While knowledge connected to social structures such as communities can strongly influence behavioral intentions (Bandura, 2004), there must be good reasons for individuals to participate in such communities. The research lists purposive value, self-discovery, maintaining interpersonal interconnectivity, social enhancement, and entertainment value (Dholakia, Bagozzi and Pearo, 2004). While such motivational aspects are fairly easy to establish for positive communities such as travel communities (cf. Aschoff and Schwabe, 2014), it may be hard to onboard people solely based on a preventative intention. Thus:

Objective 3: *Engage learners in cyber-security communities.*

Design challenge 3: *Identify strong motivators for individuals to engage in positive communities based on their current demands.*

It is hard to change individuals' attitudes, and not every information source is useful for this purpose. For instance, it can be shown that knowledge about vulnerability to a threat (i.e. the likelihood that it will occur) does not change attitudes, but that gaining knowledge of a threat's severity does (De Hoog, Stroebe and de Wit, 2007). However, while this seems plausible in a healthcare setting (i.e. the severity of a heart attack is comparable among all people), it creates challenges in cyber-security as a threat's severity strongly depends on the actual setting in question. For instance, while a two-day outtake of the core IT infrastructure may be annoying and costly for one company, it could mean the immediate termination of business for another (e.g. a bank). Thus, in contrast to fear mongering, communicating about a threat's severity is crucial and should be done specific to the context an individual operates in. The same is true for threat likelihood, which can influence behaviors but not attitudes. Here too, the likelihood depends on many factors, such as attack surface or whether or not an attack is targeted. Thus:

Objective 4: *Tailor all knowledge on threat severity and threat likelihood to the individual learner.*

Design challenge 4: *Determine a threat's individual and organizational significance and align the knowledge transfer to it.*

Especially small and medium-sized companies (SMEs) have limited capabilities to defeat cybercrime and often lack specific personal and knowledge, but still face the full spectrum of threats (Keller et al., 2005). Keller et al. (2005) pointed out more than a decade ago that more than 50% of breaches were caused by unintentional actions by internal personnel. This figure has hardly changed since. Thus, if the specific competences are not available in these small companies, inter-organizational exchange is key. While this influence (mimicking competitors) is a known significant influential factor concerning management beliefs on cyber-security threats (Barton et al., 2016), this exchange of information can also broaden views on cyber-security when performed with other (more unrelated) businesses. This approach may sound unrealistic, but has proven to work in the past (e.g. for the spread of management systems such as lean management). Thus, we formulate our last design objective:

Objective 5: *Establish broad inter-organizational knowledge exchange.*

Design challenge 5: *Provide means to share security-related information without disclosing sensitive data and without losing face.*

4.1 A Knowledge Management Perspective on the Solution Objectives

Since the abstract design goal focuses on knowledge aspects, we use a common knowledge management framework to evaluate our objectives and challenges in terms of completeness. Table 4 maps the design objectives and challenges to widely adopted notion of knowledge management (process view): *knowledge creation, storage and retrieval, distribution, and application* (Alavi and Leidner, 2001).

		Creation	Storage & retrieval	Distribution	Application
Obj 0	*Theory based design of learning*			x	
Chal 0	*Tradeoff between different constructs*			x	
Obj 1	*Align knowledge and self-efficacy*	x			
Chal 1	*Self-efficacy-based content distribution*			x	
Obj 2	*Self-monitoring and self-guided learning*		x	x	x
Chal 2	*Measuring the progress of behavioral change*				x
Obj 3	*Communities*		x	x	
Chal 3	*Motivation to engage in communities*				
Obj 4	*Tailored knowledge*	x			
Chal 4	*Distribute knowledge according to the demand*		x	x	
Obj 5	*Inter-organizational exchange*			x	
Chal 5	*Abstraction from specific case*	x	x		

Table 4: Challenges and Objectives Mapped to Knowledge Management Concepts

As we can see in the table, all knowledge management categories are addressed by the suggested design objectives and challenges. However, given cyber-security's unique behavioral properties, we argue that a design solution (although following the abstract concept of a knowledge management system) must be also highly specialized. Taking knowledge creation as an example (i.e. discovering previously unknown knowledge as well as internalizing existing knowledge) (cf. Alavi and Leidner, 2001), we expect that a knowledge source must detach specific knowledge from the given context (externalize and abstract from the context), while a learner must internalize the knowledge and attach it to their context. While this may be true for any knowledge transfer, it is particularly difficult here, since the knowledge (e.g. about a threat) must not only be attached to a target company's technical specificities, but also to its culture and value system, as well as to a learner's individual belief system. Given the still large number of breaches, despite the high availability of abstract knowledge, we expect that these adaptation processes do not function correctly, and call for further research into the topic.

Summing up our discussion of the solutions space exploration, the main challenge seems to be the specific demand to abstract from context-specific knowledge, store, share, and transport this knowledge and then de-abstract it (thus, connecting it to the target context) before learning takes place. These transfers must happen intra-organizationally and inter-organizationally, to allow for a maximum reach of security-relevant knowledge. Further, the learning cycles and the adoption of learning goals to a specific content and a learner's personal development must be managed. Given the tight budgets, the only way we see to cope with this problem is to automate these mechanisms as far as possible. These issues needs to be addressed in future research.

5 Conclusion

We have looked into the behavioral aspects of individuals' approaches to cyber-security. Given the many successful attacks and unintended breaches caused 'by accident' or even planned malicious behaviors, cyber-security is in crisis. We identified six design objectives to a cyber-security training system, inspired by the models and theories that explain mechanisms of individuals' behaviors. We thereby answered the research questions and prepared researchers to answer Karjalainen and Siponen's (2011) call to explore cyber-security training from (1) a validation of training perspective, (2) critical-level pedagogical principles, and (3) an experiential and collaborative perspective. The identified design objectives especially address the first and second part of this call for research, since they (1) target measurable variables, provided by the underlying behavioral models, and (2) help to select the basic curriculum entities and goals of training and transmission taught with a self-learning and self-directed approach.

While in this study we have done a rigorous literature review, it has also limitations. First, every literature review may miss important publications. We sought to mitigate the risk by including several databases and meta-search engines, keeping the search query broad, and did not restrict the search to a particular timespan. Further, we focused on articles that were subject to substantial scientific discourse and included further articles based on forward-search and backward-search. Second, the presented design objectives are still tentative, since empirical support is currently not available. While this is subject to future research, we could provide explanatory and conceptual grounding for both the problem description and for the solutions objective.

References

Ahmad, A., S. B. Maynard and S. Park. (2014). “Information security strategies: towards an organizational multi-strategy perspective.” *Journal of Intelligent Manufacturing; London*, *25*(2), 357–370.

Ajzen, I. (1985). “From intentions to actions: A theory of planned behavior.” In: *Action control* (pp. 11–39). Springer.

Ajzen, I. (1991). “The theory of planned behavior.” *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Alavi, M. and D. E. Leidner. (2001). “Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues.” *MIS Quarterly*, *25*(1), 107–136.

Aschoff, F. R. and G. Schwabe. (2014). “Online Travel Communities: A Self-Determination Theory Approach.” In: *Virtual Communities: 2014* (pp. 50–66). Routledge.

Atoum, I., A. Otoom and A. A. Ali. (2017). “Holistic Cyber Security Implementation Frameworks: A Case Study of Jordan.” *International Journal of Information, Business and Management; Chung-Li*, *9*(1), 108–118.

Bandura, A. (2004). “Health promotion by social cognitive means.” *Health Education & Behavior*, *31*(2), 143–164.

Barton, K. A., G. Tejay, M. Lane and S. Terrell. (2016). “Information system security commitment: A study of external influences on senior management.” *Computers & Security*, *59*, 9–25.

Baskerville, R., P. Spagnoletti and J. Kim. (2014). “Incident-centered information security: Managing a strategic balance between prevention and response.” *Information & Management*, *51*(1), 138–151.

Ben-Asher, N. and C. Gonzalez. (2015). “Effects of cyber security knowledge on attack detection.” *Computers in Human Behavior*, *48*, 51–61.

Boss, S. R., L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss. (2009). “If someone is watching, I’ll do what I’m asked: mandatoriness, control, and information security.” *European Journal of Information Systems; Basingstoke*, *18*(2), 151–164.

Chen, C. C., R. S. Shaw and S. C. Yang. (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; Morehead*, *24*(1), 1–14.

Chen, Y. and F. Zahedi. (2016). “Individual’s Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China.” *Management Information Systems Quarterly*, *40*(1), 205–222.

Craigen, D., N. Diakun-Thibault and R. Purse. (2014). “Defining cybersecurity.” *Technology Innovation Management Review*, *4*(10).

CyberEdge Group. (2016). “2016 Cyberthreat Defense Report.” Retrieved from https://webroot-cms-cdn.s3.amazonaws.com/4814/5954/2435/2016_cyberedge_group_cyberthreat_defense_report.pdf

D’arcy, J. and T. Herath. (2011). “A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.” *European Journal of Information Systems; Basingstoke*, *20*(6), 643–658.

Davis, F. D. (1989). “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.” *MIS Quarterly*, *13*(3), 319–340.

De Hoog, N., W. Stroebe and J. B. de Wit. (2007). *The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis.* Educational Publishing Foundation.

Dholakia, U. M., R. P. Bagozzi and L. K. Pearo. (2004). “A social influence model of consumer participation in network-and small-group-based virtual communities.” *International Journal of Research in Marketing*, *21*(3), 241–263.

Dinev, T. and Q. Hu. (2007). “The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies.” *Journal of the Association for Information Systems; Atlanta*, *8*(7), 386-392,394-408.

Endsley, M. R. (1995). "Toward a theory of situation awareness in dynamic systems." *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64.

Flores, W. R., E. Antonsen and M. Ekstedt. (2014). "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture." *Computers & Security*, *43*, 90–110.

Franke, U. and J. Brynielsson. (2014). "Cyber situational awareness – A systematic review of the literature." *Computers & Security*, *46*, 18–31.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier New York.

Goldkuhl, G. (2004). "Design theories in information systems-a need for multi-grounding." *JITTA: Journal of Information Technology Theory and Application*, *6*(2), 59.

Gordon, L. A., M. P. Loeb, W. Lucyshyn and L. Zhou. (2015). "The impact of information sharing on cybersecurity underinvestment: A real options perspective." *Journal of Accounting and Public Policy*, *34*(5), 509–519.

Gregor, S. and D. Jones. (2007). "The anatomy of a design theory." *Journal of the Association for Information Systems*, *8*(5), 312.

Herath, T. and H. R. Rao. (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of Information Systems; Basingstoke*, *18*(2), 106–125.

Hevner, A., S. March, J. Park and S. Ram. (2004). "Design Science in Information Systems Research." *Management Information Systems Quarterly*, *28*(1).

Hevner, A. R. (2007). "A three cycle view of design science research." *Scandinavian Journal of Information Systems*, *19*(2), 4.

Imgraben, J., A. Engelbrecht and K.-K. R. Choo. (2014). "Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users." *Behaviour & Information Technology*, *33*(12), 1347–1360.

Ion, I., R. Reeder and S. Consolvo. (2015). ""... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices." In: *SOUPS* (pp. 327–346).

Jeske, D. and P. van Schaik. (2017). "Familiarity with Internet threats: Beyond awareness." *Computers & Security*, *66*, 129–141.

Junger, M., L. Montoya and F.-J. Overink. (2017). "Priming and warnings are not effective to prevent social engineering attacks." *Computers in Human Behavior*, *66*, 75–87.

Karjalainen, M. and M. Siponen. (2011). "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches." *Journal of the Association for Information Systems*, *12*(8).

Keller, S., A. Powell, B. Horstmann, C. Predmore and M. Crawford. (2005). "Information Security Threats and Practices in Small Businesses." *Information Systems Management; Abingdon*, *22*(2), 7–19.

Kruger, J. and D. Dunning. (1999). "Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments." *Journal of Personality and Social Psychology*, *77*(6), 1121.

Lebek, B., J. Uffen, M. Neumann, B. Hohler and M. H. Breitner. (2014). "Information security awareness and behavior: a theory-based literature review." *Management Research Review: MRN; Patrington*, *37*(12), 1049–1092.

Lee, J. S., J. Pries-Heje and R. Baskerville. (2011). "Theorizing in design science research." In: *International Conference on Design Science Research in Information Systems* (pp. 1–16). Springer.

Logan, P. Y. and A. Clarkson. (2005). "Teaching Students to Hack: Curriculum Issues in Information Security." In: *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* (pp. 157–161). New York, NY, USA: ACM.

Maddux, J. E. and R. W. Rogers. (1983). "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change." *Journal of Experimental Social Psychology*, *19*(5), 469–479.

McAffee, Part of Intel Security. (2016). "Hacking the Skills Shortage." Retrieved from https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

"M-Trends 2017 Cyber Security Trends." (2017). Retrieved from https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Öğütçü, G., Ö. M. Testik and O. Chouseinoglou. (2016). "Analysis of personal information security behavior and awareness." *Computers & Security*, *56*, 83–93.

Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac and T. Zwaans. (2017). "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies." *Computers & Security*, *66*, 40–51.

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

Peffers, K., T. Tuunanen, M. A. Rothenberger and S. Chatterjee. (2007). "A design science research methodology for information systems research." *Journal of Management Information Systems*, *24*(3), 45–77.

Pfleeger, S. L. and D. D. Caputo. (2012). "Leveraging behavioral science to mitigate cyber security risk." *Computers & Security*, *31*(4), 597–611.

Pompon, R. (2016). "Assume Breach." In: *IT Security Risk Control Management* (pp. 13–21). Springer.

Posey, C., T. L. Roberts, P. B. Lowry and R. T. Hightower. (2014). "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders." *Information & Management*, *51*(5), 551–567.

Purkait, S. (2012). "Phishing counter measures and their effectiveness - literature review." *Information Management & Computer Security; Bradford*, *20*(5), 382–420.

Quigley, K., C. Burns and K. Stallard. (2015). ""Cyber Gurus": A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection." *Government Information Quarterly*, *32*(2), 108–117.

Rimal, R. N. (2000). "Closing the knowledge-behavior gap in health promotion: the mediating role of self-efficacy." *Health Communication*, *12*(3), 219–237.

Rocha Flores, W. and M. Ekstedt. (2016). "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness." *Computers & Security*, *59*, 26–44.

Safa, N. S., M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani and T. Herawan. (2015). "Information security conscious care behaviour formation in organizations." *Computers & Security*, *53*, 65–78.

Safa, N. S. and R. Von Solms. (2016). "An information security knowledge sharing model in organizations." *Computers in Human Behavior*, *57*, 442–451.

Sikula, N. R., J. W. Mancillas, I. Linkov and J. A. Mcdonagh. (2015). "Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments." *Environment Systems & Decisions; New York*, *35*(2), 219–228.

Sohrabi Safa, N., R. Von Solms and S. Furnell. (2016). "Information security policy compliance model in organizations." *Computers & Security*, *56*, 70–82.

Soomro, Z. A., M. H. Shah and J. Ahmed. (2016). "Information security management needs more holistic approach: A literature review." *International Journal of Information Management*, *36*(2), 215–225.

Stafford, M. C. and M. Warr. (1993). "A reconceptualization of general and specific deterrence." *Journal of Research in Crime and Delinquency*, *30*(2), 123–135.

Thamsirarak, N., T. Seethongchuen and P. Ratanaworabhan. (2015). "A case for malware that make antivirus irrelevant." In: *2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)* (pp. 1–6).

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

Tsohou, A., M. Karyda, S. Kokolakis and E. Kiountouzis. (2015). "Managing the introduction of information security awareness programmes in organisations." *European Journal of Information Systems; Basingstoke*, *24*(1), 38–58.

Usman, A. K. and M. H. Shah. (2013). "Critical Success Factors for Preventing e-Banking Fraud." *Journal of Internet Banking and Commerce; Ottawa*, *18*(2), 1–15.

Vom Brocke, J., A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven and others. (2009). "Reconstructing the giant: On the importance of rigour in documenting the literature search process." In: *ECIS* (Vol. 9, pp. 2206–2217).

Webster, J. and R. T. Watson. (2002). "Analyzing the past to prepare for the future: Writing a literature review." *MIS Quarterly*, xiii–xxiii.

Woon, I., G.-W. Tan and R. Low. (2005). "A Protection Motivation Theory Approach to Home Wireless Security." *ICIS 2005 Proceedings*.

Zafar, H., A. Randolph and N. Martin. (2017). "Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior." *AIS Transactions on Human-Computer Interaction*, *9*(1), 59–74.