Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Future directions for behavioral information security research

Robert E. Crossler [a,*], Allen C. Johnston [b], Paul Benjamin Lowry [c], Qing Hu [d], Merrill Warkentin [a], Richard Baskerville [e]

[a] Mississippi State University, Management and Information Systems, PO Box 9581, 302 McCool Hall, Mississippi State, MS 39762, USA
[b] University of Alabama at Birmingham, 1530 3rd Avenue South, School of Business, Birmingham, AL 35294, USA
[c] City University of Hong Kong, P7912 Academic Building I, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China
[d] Iowa State University, 2211 Gerdin Business Building, Ames, IA 50011, USA
[e] Georgia State University, PO Box 4015, Atlanta, GA 30302-4015, USA

ARTICLE INFO

Article history:
Received 31 May 2012
Received in revised form
3 September 2012
Accepted 26 September 2012

Keywords:
Information security
Future research
Behavioral information security
Research challenges
Deviant security behavior

ABSTRACT

Information Security (InfoSec) research is far reaching and includes many approaches to deal with protecting and mitigating threats to the information assets and technical resources available within computer based systems. Although a predominant weakness in properly securing information assets is the individual user within an organization, much of the focus of extant security research is on technical issues. The purpose of this paper is to highlight future directions for Behavioral InfoSec research, which is a newer, growing area of research. The ensuing paper presents information about challenges currently faced and future directions that Behavioral InfoSec researchers should explore. These areas include separating insider deviant behavior from insider misbehavior, approaches to understanding hackers, improving information security compliance, cross-cultural Behavioral InfoSec research, and data collection and measurement issues in Behavioral InfoSec research.

1. Introduction

Information Security (InfoSec) research is far reaching and includes technical, behavioral, managerial, philosophical, and organizational approaches that address the protection and mitigation of threats to information assets (Zafar and Clark, 2009). Though some of the Information Systems research in the InfoSec field has considered socio-philosophical concerns or socio-organizational concerns, it has primarily focused on technical issues concerning the design and implementation of security subsystems (Choo, 2011; Zafar and Clark, 2009), such as advanced technical approaches to prevent intrusion into organizational systems (Hansen et al., 2007), detection of denial of service attacks (Zhi-jun et al., 2012), and more advanced solutions for firewall protection (Ayuso et al., 2012). Although these technical, externally focused efforts are important, one area that is a predominant weakness in properly securing information assets is the individual user within an organization (Leach, 2003; Posey et al., 2011b; Sasse et al., 2001; Stanton et al., 2005; Vroom and von Solms, 2004; Warkentin and Willison, 2009). This is a particularly important problem because researchers estimate that nearly half of intrusions and security violations occur from within an organization by organizational insiders (Baker et al., 2010; Richardson, 2011). Until recently, research exploring the operational aspect of information security has been lacking.

* *Corresponding author*. Tel.: +1 662 325 0288; fax: +1 662 325 8651.
E-mail addresses: rob.crossler@msstate.edu (R.E. Crossler), ajohnston@uab.edu (A.C. Johnston), Paul.Lowry.PhD@gmail.com (P.B. Lowry), qinghu@iastate.edu (Q. Hu), m.warkentin@msstate.edu (M. Warkentin), baskerville@acm.org (R. Baskerville).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.09.010

Behavioral InfoSec research is a subfield of the broader InfoSec field that focuses on the behaviors of individuals which relate to protecting information and information systems assets (Fagnot, 2008; Stanton et al., 2006), which includes computer hardware, networking infrastructure, and organizational information. Recently, a number of studies have been published about the behaviors of individuals in protecting these assets. These studies include those that provide insight into insider abuse of information systems (Siponen and Willison, 2009; Willison, 2006; Willison and Backhouse, 2006), as well as applying General Deterrence Theory (GDT) to understand human behavior as it relates to computer crime and intentional abuse (Straub and Nance, 1990; Straub and Welke, 1998). Further studies have adapted Protection Motivation Theory (PMT) to understand the behaviors of individuals when it comes to the performance of a number of security measures, such as the use of anti-malware software (Johnston and Warkentin, 2010; Lee and Larsen, 2009; Liang and Xue, 2010), compliance with security policies (Herath and Rao, 2009b; Ifinedo, 2012), backing up data (Crossler, 2010), properly securing home wireless networks (Woon et al., 2005), and adoption of anti-plagiarism software (Lee, 2011). Beyond PMT, other empirical studies exist that investigate behavioral factors that affect such areas as security policy compliance (Bulgurcu et al., 2010; Herath and Rao, 2009a; Hu et al., 2011a, 2012; Siponen and Vance, 2010; Warkentin et al., 2011a), information systems misuse (D'Arcy and Hovav, 2007; D'Arcy et al., 2009; Posey et al., 2011b), and computer abuse (Lee et al., 2004; Posey et al., 2011a).

Even with the number of Behavioral InfoSec research studies being published, significant challenges still remain that must be overcome as this research stream moves forward. The ensuing paper identifies these challenges and presents approaches that could be utilized to address them. Resulting from this analysis are future directions that Behavioral InfoSec researchers should explore.

2. Identifying future behavioral information security research directions

In this section, we present the methodology utilized to identify the future directions of Behavioral InfoSec research. The process leveraged input from the International Federation for Information Processing (IFIP) Working Group 8.11/11.13 on Information Systems Security Research via contributions from participants of the Dewald Roode Information Security Workshop, which is prominent in promoting this area of research, as well as other scholars that are members of the IFIP Working Group. Five themes for future research were identified through this process.

Prior to the 2011 Dewald Roode Information Security Workshop, scholars were asked to submit research ideas that could drive the future of Behavioral InfoSec projects. A total of 13 ideas were submitted. These ideas were placed into five separate groupings by the program chair of the workshop based on commonalities in the topics presented, with three ideas per group. Two of the proposed directions for research were included in two groupings due to the breadth of the idea and how it overlapped with multiple topics. Five groups were created to keep groups to a reasonable size of five to seven participants per group. At the conclusion of the workshop, participants were randomly assigned to one of the five groups where they were provided with one of the compiled lists. A group facilitator then led a discussion about future projects that would advance Behavioral InfoSec research beyond its current *status quo*. After the workshop, the facilitators of these groups summarized the discussions. The summarized lists were then analyzed and grouped into similar categories.

Following this, other scholars in the Behavioral InfoSec and Information Systems community were consulted regarding their insight to future research directions for Behavioral InfoSec research. These insights were combined with the categories identified from the workshop and expanded upon in this paper.

3. Future behavioral information security research directions

In this section, we propose and discuss several areas of interesting future Behavioral InfoSec research resulting from the IFIP Working Group's members' discussions and analyses as well as methodological challenges that need to be faced. The research areas include the following categories:

- Separating insider deviant behavior from insider misbehavior
- Unmasking the mystery of the hacker world
- Improving information security compliance
- Cross-cultural InfoSec research.

The methodological challenges include data collection and measurement issues.

3.1. *Research areas*

3.1.1. *Separating insider deviant behavior from insider misbehavior*

In the Behavioral InfoSec academic literature and industry surveys of IT managers, it is well acknowledged that people within organizations are still the weakest link in the defense against internal and external threats to organizational digital assets—in spite of the significant advances in protective technologies and organizational procedures and policies related to information security (Hu et al., 2012; Warkentin and Willison, 2009). Many of the headline security breach incidents would have not been possible without some intentional or unintentional actions by the insiders. In fact, surveys suggest that more information security breaches are caused by the actions of internal employees than by outside hackers (Baker et al., 2010; Richardson, 2011).

The insider actions that cause direct or indirect threats to organizational digital assets can be classified into two categories: those that are intentional, often labeled as deviant behavior—such as sabotage, stealing, and industrial or political espionage—and those that are unintentional, often labeled as misbehavior—such as selecting a simple password, visiting non-work related websites using corporate computers, inadvertently posting confidential data onto unsecured servers or websites, or carelessly clicking on

phishing links on emails and websites (Guo et al., 2011; Stanton et al., 2005; Willison and Warkentin, 2013). A significant number of IS studies have been conducted investigating the effectiveness of deterrence (D'Arcy et al., 2009; D'Arcy and Herath, 2011; D'Arcy and Hovav, 2007; Herath and Rao, 2009a; 2009b; Lee et al., 2004; Siponen and Willison, 2007; Straub and Nance, 1990; Straub and Welke, 1998; Theoharidou et al., 2005) on deviant insider behavior. Recently, other cognitive and psychological factors have been included in the increasingly complex insider behavior models, such as rational choice and beliefs (Bulgurcu et al., 2010), neutralization (Siponen and Vance, 2010), fear (Johnston and Warkentin, 2010), self-control and moral beliefs (Hu et al., 2011a; Myyry et al., 2009), accountability (Vance et al., 2011, 2012a), disgruntlement (Willison and Warkentin, 2013), and leadership and organizational culture (Hu et al., 2012).

The findings of such studies have significantly advanced our understanding of insider motivations and psychological processes when evaluating whether or not to comply with established information security procedures and policies. However, in most of these studies no attempt was made to differentiate between the survey samples drawn from those who intentionally violate the procedures and policies and drawn from those who unintentionally violate them. Differentiating these samples is important as the causes of intentional violations of policies likely differ from the causes of unintentional violations, although the outcomes can be just as damaging. For example, deviant insider behavior can cause significant direct damages to organizations, such as loss of revenue, weakened competitive positions, and loss of credibility. On the other hand, insider misbehavior can be equally as damaging, but most often indirectly by creating security weakness that allow outside hackers to invade internal systems, such as infecting corporate computers with Trojan viruses and spyware that allow hackers to bypass the firewall defense and access confidential data.

The mixing of these two categories of insiders can significantly limit the effectiveness and even applicability of some of the recommended remedies in these studies. For example, information security training aimed at improving awareness and efficacy (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath and Rao, 2009a, 2009b; Straub and Nance, 1990; Straub and Welke, 1998) or a rule- and goal-oriented organizational culture (Hu et al., 2012) might not be effective for preventing the deviant behavior of the insiders who are motivated to harm the organization or to benefit themselves. Moreover, deterrence (D'Arcy et al., 2009; Herath and Rao, 2009a, 2009b; Straub and Nance, 1990) and neutralization (Siponen and Vance, 2010) mechanisms might not be applicable to those insiders who violate the procedures and policies due to their own sloppiness and ignorance. Similarly, the findings in studies on information security policy compliance with samples that include those insiders who have the intention to violate security policies may be as contaminated and unreliable as the findings of studies on information security policy violation with samples that include those who are merely careless or ignorant.

Thus, it is clear that a comprehensive information security program must effectively investigate the range of behaviors from merely careless or uninformed nonvolitional actions to volitional (but not malicious) behaviors to malicious acts from insiders (Willison and Warkentin, 2013). Future InfoSec research in the organizational context should specify where behaviors are at on the continuum between nonvolitional and malicious, match behavior with motivation, and use more focused subjects for a particular research. Volitional but not malicious behavior could be better studied with subjects who have no intention to violate established information security policies, whereas malicious behavior might be better studied with subjects who do have the intention or at least are likely to violate established information security policies. The difficulty in executing this strategy is categorizing the subjects before administrating the survey or other measurement instruments. One possible approach is to screen the subjects based on their moral beliefs and self-control scores—two significant indicators of deviant behavior in organizations (Hu et al., 2011a; Myyry et al., 2009).

3.1.2. *Unmasking the mystery of the hacker world*

The current IS research on information security has been criticized as focusing only on the low hanging fruit—insiders who may or may not have intention to harm the organization by violating the established information security procedures and policies (Mahmood et al., 2010). As discussed previously, the puzzle of information security is comprised of many opposing but interwoven pieces such as technology versus people, insiders versus outsiders, and deviant behavior versus misbehavior. One major piece that is clearly a valuable high-hanging fruit that has not been adequately studied by IS scholars is the mysterious world of computer hackers. The study of computer hackers is made even more difficult with the various definitions of hackers that exist. At a high level, hackers refer to those people who attack an organization's information systems infrastructure for a variety of reasons, and can be viewed as state hackers, terrorists, non-state hackers/organized crime, disgruntled employees/insider attackers, hobbyists, script kiddies, hacktivists, and legitimate penetration testers (Nicholson et al., 2012). Some research differentiates between hackers and crackers with crackers being those people who hack into systems to damage people or companies via the Internet (Barber, 2001). However, in the 1980s law enforcement began to use the term hackers for people who met this definition (Hollinger, 1991).

The first challenge in researching the hacker community is accurately defining the group of people that are being investigated. Each type of hacker will have their own reasons why they perform the behaviors they do, making proper definition of the context crucially important. Although not explicitly stated as such, existing hacker research has focused on providing insight and understanding to hackers who could be classified as non-state hackers or criminal hacking (Hu et al., 2011b; Schell et al., 2002; Taylor, 1999; Young et al., 2007), and hacking in general (Bossler and Burruss, 2011). One article provides the foundation of investigating these differences by providing the evolutionary stages that young hackers go through of starting with "hacking for fun," progressing to a "do no harm" approach and finally resulting in hacking for survival or for profit (Hu et al., 2011b). An avenue for future research would be to expand on this approach and provide

more differentiation on the behavioral motivations of these different types of hackers.

Regardless of the type of hacker being studied, the primary challenge in hacking research is gaining access. By nature, hackers are not easily identifiable and hacking activities are conducted in secret. Even though the hackers and hacking incidents have dominated the headline news in the last decade, few rigorously conducted hacker studies have been published, and most of our understanding about computer hackers comes from descriptive accounts and reporting (e.g., Barber, 2001; Levy, 2001; Schell et al., 2002; Taylor, 1999). Although many scholars have attempted to study hackers and hacking behavior (e.g., Bossler and Burruss, 2011; Halbert, 1997; Hollinger, 1991; Roberts, 1995; Rogers et al., 2006a, 2006b; Yar, 2005), almost none used known hackers as the subjects of study but relied on the general population such as college students.

We are aware of only a few studies that used known hackers as the informants, such as Young et al. (2007) and Hu et al. (2011b), but most of the research remains at the exploratory stage with limited sample sizes. Strong theoretical foundations and rigorous research methodologies are lacking from the extant hacker research literature. To address the theoretical shortcomings, criminological theories could provide a rich foundation for this line of research, such as the situational action theory (Wikström, 2004, 2006) or the idea of routine activity theory (Cohen and Felson, 1979). The main challenge of hacker research, however, remains the identification and access to the hacker population, which will likely limit scholars' ability to test and validate theories. Innovative research methodologies are strongly desirable. Regardless of the difficulties, gaining a rich understanding of hacker behavior could lead to native theories in the information security research field that could have a profound impact for a number of related academic disciplines.

3.1.3. *Improving information security compliance*

Fear-based persuasive communication and fear-related models pertaining to security compliance are increasingly important to consider, because fear is an underlying driver of Rogers' (1983) Protection Motivation Theory (PMT) that has been examined in recent studies within the Behavioral InfoSec domain (Herath and Rao, 2009b; Ifinedo, 2012; Johnston and Warkentin, 2010; Liang and Xue, 2010; Posey et al., 2011c). To date, fear appeal studies have only scratched the surface of the potential of fear as a motivator for security compliance, with numerous issues surrounding its application still left unexplored. For instance, questions remain as to the appropriate context and alignment of fear-based persuasive communication with interests and perspectives of the audience of message recipients. Further, we still know little about the circumstances from which individuals feel fearful and the characteristics of the individuals that may serve to accentuate or diminish the emotion of fear in security compliance situations. For example, an end user might fear being caught for policy violations more than they fear having their personal information compromised, and this determination may be dependent upon the personality type or some other perceptual disposition held by the user. The disparate nature of the influence of fear on individual security outcomes underscores the difficulty in conducting research in this area, but also offers a hope of opportunity for a meaningful contribution to knowledge.

Further complicating the study of fear-based persuasive messages is the connotation of the word 'fear.' In a Behavioral InfoSec context, is fear as powerful of a motivator as it is in the context of the extant research from which this construct has been adapted? It is hard to imagine that the fear someone experiences when faced with threats to data or computer systems is at the same magnitude as the fear of being diagnosed with cancer. The emotion experienced in these two settings may be completely different and have different characteristics, such as its rate of dissipation, its potential to interact with other factors, its unique manifestation and intensity in individuals, its relationship to coping appraisal, and how it is translated into behavior. Accordingly, we believe that fear is likely a multi-faceted construct that can manifest itself in different degrees that are highly relevant to Behavioral InfoSec research.

Fear appeals also present some measurement issues that extend the discussion above. Behavioral InfoSec research that captures perceptions of fear does so via a survey methodology or embedded within a lab experiment. For InfoSec fear appeals to be effective, however, the appeal must successfully manipulate the neural regions of the message recipient's brain responsible for cognitively processing perceptions of threat and efficacy. Threat appraisal is a cognitive assessment of vulnerability which may or may not be associated with the intense affective response to immediate danger; while coping appraisal is a parallel cognitive mediating process in which the message recipient engages in an assessment of his or her own ability to cope with the threat (self-efficacy) and of the efficacy of the recommended response. In the studies to date, subjects cognitively assess the instrument items and their perceptions in cognitive terms, not in the moment of fear occurrence, but rather as a self-assessment of a perspective determined post-stimulus (e.g., Anderson and Agarwal, 2010; Herath and Rao, 2009b; Ifinedo, 2012; Johnston and Warkentin, 2010; Liang and Xue, 2010). Future research could further utilize fMRI, EEG, or other physiological techniques in a laboratory setting to better capture the extent to which fear is realized in its affective (emotional) and then cognitive forms.

This raises another confound in whether a clearly artificial laboratory setting can accurately represent the fear that users experience in the moment their information is compromised or when they are caught violating information security policies—both situations obviously cause higher levels of fear than in a hypothetical scenario situation presented in the laboratory. Bringing together the different approaches and utilizing a number of different methodologies in a fear appeals research stream would greatly increase our understanding of the impact that fear has on InfoSec-related outcomes, including compliance with information security polices or recommendations.

Another avenue of research would investigate the dynamics of fear over time, as users react to events they encounter when interacting with technologies that may pose perceived threats. One interesting study (Vance et al., 2012b) investigates the impact on users of a real-time dynamic fear appeal based on their current actions. When the system

assessed that threat levels are increasing, the user is offered more intense warnings.

Beyond the work involving fear appeals, we can look to other established behavioral modifiers, such as deterrence, to aid in our understanding of information security compliance. One avenue to explore is how organizational justice influences compliance (Posey et al., 2011a; Willison and Warkentin, 2013). For example, if individuals believe that their organization is fair in how they apply their IT policies, it may be more likely that people will comply with these policies. As researchers begin to explore these issues, it will be possible to gain a better understanding of the individuals who are most likely to violate policies and their rationale for violating policies, and to intervene before they engage in detrimental behavior. In doing so, researchers can uncover more effective ways to communicate and deliver IT policies and determine whether training on the efficacy and role of IT policies increases compliance.

3.1.4. *Cross-cultural InfoSec research*

One of the biggest issues and limitations of Behavioral InfoSec research is that the majority of it has been conducted in Western cultures, with occasional studies being conducted in Asia and elsewhere. Most of the rest of the world has been overlooked; and little has been done to examine cross-cultural considerations involved with insider behavior, IT security compliance, hacking, security violations, and so forth. These are particularly important considerations because culture likely has a direct impact on these phenomena. Current studies may need to be adapted to account for cross-cultural differences such as uncertainty avoidance, collectivism-individualism, and power distance relationships. These cross-cultural differences have been shown to be strong and salient in other IT contexts (Lowry et al., 2011, 2010; Posey et al., 2010; Srite and Karahanna, 2006; Zhang and Lowry, 2008; Zhang et al., 2007), so there is every reason to believe they are likely to apply in a Behavioral InfoSec context. By way of illustration, we review some of the basic concepts of culture from the literature, and explain how these could impact Behavioral InfoSec topics and issues.

Per Zhang and Lowry (2008), *uncertainty avoidance* is the extent to which the members of a culture feel threatened by uncertain or unknown situations. Denmark and Singapore are examples of low uncertainty-avoidance national cultures; whereas, Japan is an example of high-uncertainty avoidance. Given their propensity to shun uncertainty, it is likely that a Japanese end-user is less likely to fall prey to phishing emails whereas people who are more open to uncertainty might be more likely to be victimized by a phishing attack.

Meanwhile, *individualism* describes cultures in which the ties between individuals are loose. *Collectivism* describes cultures in which people are integrated into strong, cohesive groups that protect individuals in exchange for unquestioning loyalty (Zhang and Lowry, 2008). The US is an example of a highly individualistic national culture whereas China is an example of a highly collectivistic culture. These cultural differences—to the degree they are held by individuals living within such cultures—could clearly have a positive or negative impact on IS security behaviors in organizations. For example, stronger loyalty in collectivistic individuals could cause them to more strongly adhere to IT security policies—but only as long as this adherence is seen as loyalty. The flip side is that such a person might be less likely to report IT violations of people to whom they are loyal. Hence, individualists should be much more likely to whistle-blow severe security violations committed by key organizational members to whom they feel loyalty.

Power distance is the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally (Zhang and Lowry, 2008). An example of a low power distance national culture is Canada; an example of a high power distance culture is China. Power distance could have a dramatic effect on buy-in and acceptance of newly generated IT security policies. It is likely those who are in high-power distance cultures are more readily willing to comply with detailed policy requirements, whereas those from low-power distance cultures are likely to pick-and-choose which policies they feel they should obey.

Another way to look at culture is through Confucian dynamism. Confucian dynamism denotes the time orientation of a culture, defined as a continuum with long-term and short-term orientations as its two poles (Zhang and Lowry, 2008). National cultures that are said to be low in Confucian dynamism, or have short-term orientations, are the US and Canada; national cultures that are high in Confucian dynamism, or have long-term orientations, are China and Japan. Such differences in time orientation could have profound effects for how leaders in organizations strategically consider their security architecture for the longer term. If true, it would be expected that IT leaders with a longer view would engage in more advanced, long-term planning that would focus on a scalable, highly secure architecture and policies for improving IT security. Those with a more short-term view might architect less broadly and will focus on a more short-term "results" orientation.

Another cultural lens that can provide insights on Behavioral InfoSec is that of the Cultural Theory of risk (Douglas, 1992). This theory attempts to explain societal conflict over risk. Because of the Cultural Theory's focus on risk, application to the Behavioral InfoSec context could be fruitful. For example, part of the premise of the Cultural Theory is that social organization structures cause individuals to have perceptions that reinforce those structures versus alternative structures. Hence, it would be interesting to use this theory to predict how organizational structures affect risk perceptions about security.

Providing further insight to the influence that culture has on Behavioral InfoSec would be to measure individual differences as they relate to each of the items identified by Hofstede (2001). Hofstede's measures generalize an entire country to culturally have certain traits as compared to other countries. However, individuals within each country vary in their own traits in that particular area (Srite and Karahanna, 2006). Relying on a country level assessment of individual's culture could result in inaccurate findings if the individual's propensity to that cultural value did not match the overall values of the country. Further, by measuring individual attributes and how they display the cultural trait, insight could be provided that would otherwise be missed. For example in a cross-

cultural study within group as well as across group analyses could be performed on cultural traits. This would provide stronger empirical support for differences found in individuals instead of differences across countries in general.

3.2. Methodological challenges

One of the common themes in the discussion above is the need for better ways to collect and measure security related data (Warkentin et al., 2011b, 2012a). In this section we describe data collection and measurement issues faced by Behavioral InfoSec researchers and suggest ways to overcome them.

3.2.1. Data collection and measurement issues

In a world where technology enables behavioral monitoring, increasingly better opportunities for measuring actual behavior exist. However, for researchers, the difficulty is acquiring access to quality data in this context. How can researchers convince companies to allow access to archival data that may be sensitive? Reports of negative behaviors might lead to legal or community relations' nightmares. Companies naturally want to avoid any publicity related to information security and negative events. Access to data about security-related events, even under conditions of anonymity, is typically (and understandably) denied. As a result, there is a dearth of actual behavior reporting in the current Behavioral InfoSec literature.

However, studies suggest that in an information security context, it is preferable to measure actual behaviors rather than intentions (Anderson and Agarwal, 2010; Mahmood et al., 2010; Straub, 2009; Warkentin et al., 2011b, 2012a). In a Behavioral InfoSec study, measuring intentions rather than behaviors for the dependent variable is especially troubling because intentions do not always lead to behaviors. For example, a person has to fail to perform a protective behavior only once in order for a threat to manifest itself. When it comes to behaviors people should be employing to protect their computers from security threats, it is the behavior that matters and not the intention to perform the behavior. Individuals are either performing the risk-mitigating behavior or they are not—intention without action may lead to a security breach. Further, research demonstrates that although people express that they are concerned about their information security, few take actions to protect the information, even at limited costs (Acquisti and Grossklags, 2004).

Although the reliance on intentions rather than actual behaviors is understandable, given the difficulties in observing and collecting actual behavior data in the context of information security, it is also limiting to theory development and theory validation. First, survey subjects naturally do not want to reveal their true responses to items they perceive might have negative consequences to their image or even job security. Therefore, social desirability, common methods bias, and acquiescence bias could be severe if the instrument and the data collection method are not well designed in advance. Anonymous and scenario-based survey design can alleviate but cannot completely eliminate these biases.

Second, even though social and behavioral studies have shown a strong correlation between behavioral intention and actual behavior (Ajzen, 2005), measuring and using data of the actual behavior should still be the ultimate goal for behavioral scholars. Thus, data collection and measuring the true dependent variable constitute the major challenge in research methodology for Behavioral InfoSec studies (Warkentin et al., 2012a).

3.2.2. Data collection and measurement solutions

Three research methodologies could offer some solution to the methodological challenge. These include qualitative methodologies, the use of longitudinal studies, and controlled laboratory and field experiment methodologies.

Qualitative methodologies, especially those that follow well-established scientific approaches, such as positivist (Eisenhardt and Graebner, 2007; Yin, 2009) and interpretive (Myers and Newman, 2007) case studies and grounded theory (Glaser and Strauss, 1967), could provide an effective method to better understand the actual motivations and behaviors of the insiders.

Although studies based on qualitative methodologies such as positivist and interpretativist case studies have started to emerge in Behavioral InfoSec research, longitudinal and laboratory studies are still rare and need to be fostered and encouraged in order to enrich the field of Behavioral InfoSec research, strengthening the theories and methodologies. The use of longitudinal studies could enable scholars to effectively collect actual behavioral data that are not possible to collect in snapshot survey research (Kim and Malhotra, 2005; Venkatesh and Davis, 2000). Research has shown that self-reported behavioral or behavioral intention data is much less accurate and reliable than actual behavioral data (Straub et al., 1995). Researchers utilizing a longitudinal study showed that the best predictor for continued system usage was past system usage as opposed to intentions (Kim and Malhotra, 2005). From a Behavioral InfoSec perspective, utilizing longitudinal studies would allow researchers to investigate the explanatory power of theories on actual behaviors over an extended period of time. One such study has been implemented to expose the impact of external factors on actual security-related behaviors over time (Warkentin et al., 2006). Insights from this research and other studies may allow for further refinement and development of our understanding on what causes people to continue performing security behaviors.

Controlled laboratory and field experiment methodologies offer another alternative venue for collecting more realistic behavioral data that can address the shortcomings of survey based research. Such an approach has been able to reveal a distinct difference between people's expressed behaviors and their actual behaviors (Acquisti and Grossklags, 2004).

Another completely new research methodology that has the potential to address the identified shortcomings is based on neurosciences such as functional magnetic resonance imaging (fMRI) and event related potential (ERP) neuroimaging technology (Dimoka, 2010, 2012; Dimoka et al., 2012). An example of an application of this research to the InfoSec domain has recently been conducted to determine the neural correlates of cognitive assessments of security threats and responses (Warkentin et al., 2012b). Another study utilizes EEGs to determine whether there is a difference in how the

brain in men and women process malware warnings differently (Anderson et al., 2012). These studies, and others like them, will offer new insights into individual behaviors and cognitions in the context of information security threats. It is imperative that Behavioral InfoSec scholars collaborate with experts in neuroscience and other disciplines to ensure scientific rigor.

Gaining access to individuals' actual behavior is one consistent challenge for Behavioral InfoSec research. One possible approach to address this challenge is to spoof real websites, such as Facebook.com, to measure actual user behavior. Because such a research approach would involve deception, extra care will be required for assuring the ethical treatment of the human subjects, but this should not prohibit researchers from exploring such unique new approaches to obtain data on actual behavior. Engaging institutional review boards in developing acceptable new approaches could not only address ethical concerns about collecting actual behavior data, it could also result in interesting (and publishable) findings regarding new data collection approaches. For example, such a spoofing approach is similar to the research being conducted in secure behavior continuance and discontinuance (Warkentin et al., 2006), in which students were encouraged to install and use anti-spyware software weekly which was not actually anti-spyware software, but merely informed the researchers whether or not the manipulation worked as intended. Participants were deceived in this scenario, but the research captured *actual* security-related behaviors.

Other research issues in Behavioral InfoSec regard developing an understanding of why people engage in unethical behaviors. People are not generally willing to admit to committing these sorts of behaviors, so it is important to identify and use the appropriate research methodologies to capture these phenomena in a way that does not depend on self-reports or admissions by subjects. Borrowing from other social science disciplines provides one resource for how to address this issue. In sociological studies, scenarios, incentives, and experiments are all used to collect behavioral data. In particular, scenarios are finding use in Behavioral InfoSec research (Siponen and Vance, 2010) and such usage could rise, as scenarios provide an opportunity to capture anti-social and unethical behavior (Pogarsky, 2004; Siponen and Vance, 2010). They do so by presenting respondents with hypothetical information and ask them what they would do in that situation. This approach allows subjects to remove their own feeling of incrimination from their responses. One study combined the scenario approach with interviews of known hackers to provide information on how to determine traits that indicate which people are more likely to become hackers (Hu et al., 2011b). This work opens the doors for future research to continue exploring ways to determine indicators of who is likely to become a criminal hacker.

Perhaps the richest source of actual security data involves gaining access to corporate data. However, as we mentioned earlier, this access can prove to be elusive as gaining access to corporate data, especially security data, can be a difficult or virtually impossible. Gaining access to this information may be possible, however, through secondary relationships with those who have such access, such as IT auditors. By removing the researcher from knowing who the company involved in security decisions is, a layer of protection may be provided that allows access to information that otherwise may not be available. Other potential ways of acquiring this sort of data may be through anonymous panels using market research and survey vendors such as Qualtrics, Zoomerang, or Empanel. One key to gaining access to corporate data is to ensure true anonymity, as companies will be much less likely to release this sort of information if they see any possibility that the information will be attributed to them.

Along these lines, Behavioral InfoSec scholars can leverage techniques by related behavioral work in deception research that is used to discover actual cases of deception and to use these as baselines (Jensen et al., 2010, 2011). In this research, subjects are invited to participate in a high-stakes experiment where incentives for lying and deception are in place (e.g., best performing team gets more money), and they are given the opportunity to naturally lie and deceive while being videotaped. In several cases, confederates within teams are used to further inspire lying and cheating. After the lying/cheating episode, all participants (whether they were honest or cheated) are given the same post-experiment instruments so that cheaters versus honest participants can be further differentiated. A similar deceptive environment with confederates acting as game masters was shown to facilitate the exposure of untrustworthy insider behavior (Ho et al., 2012). Likewise, Behavioral InfoSec researchers could create similar scenarios where high-stakes incentives are provided for organizational participants to violate actual security policies, and to capture such violations without the participants' knowledge (at least before debriefing them).

Capturing data about deception and fraud also involves a certain agreement about how to recognize such phenomena in actual settings. Other information systems theories can help provide insight into how to make such a determination. One such theory is Information Manipulation Theory (IMT), which informs us that there are different types of deception used in deceptive messages. These are manipulations of quality, quantity, relevance and clarity (McCornack, 1992; McCornack et al., 1992). By manipulating messages in these different ways, it is more likely that the receiver will be deceived simply because individuals are not very adept at detecting deception (Levine et al., 2003). This technique has been applied to understanding InfoSec behaviors such as responding to phishing attacks (Ormond and Warkentin, 2012; Wright and Marett, 2010).

For example, a researcher could design software artifacts that use IMT as a framework for detecting whether a potential insider is prone to future information abuse. In order for a system such as this to work, it would first be necessary to uncover relationships that are characteristics of known insider abusers. This could be accomplished through data mining non-security related data in employee records, from enterprise social networks, or from fraud detection networks. This information could then be used to help flag other individuals that may also pose potential insider threats. That is, data obtained from violations of policy in one area of employment relates to a propensity to commit violations in InfoSec in other areas of employment. With the emergence of enterprise social networks, sufficient data for such studies is becoming available.

These potential solutions to the methodological issues of data collection, especially the measurement of InfoSec behaviors, will serve to improve the validity of future research within our domain, and will provide practitioners with a more solid foundation from which to develop practical security solutions to the problems facing enterprise managers.

4. Discussion and conclusion

Behavioral InfoSec presents a number of opportunities to explore issues at the intersection of people, technology, and organizations. The dynamic nature of a field coupled with technology in the midst of contrary human forces leads to a challenging and ever changing target (Dlamini et al., 2009). In this paper, we have presented a number of issues that future Behavioral InfoSec researchers can tackle as they investigate these challenges. As these research issues are addressed, the InfoSec community will be better able to facilitate the establishment of more secure computing environments.

As presented in this manuscript, a number of opportunities exist to improve the existing research programs and to extend Behavioral InfoSec research into new areas. Table 1 summarizes the key themes presented in this paper, along with research that should be conducted and challenges that must be overcome in doing so. These themes should be considered from the perspective of the greater discipline of IS, of which Behavioral InfoSec research is a part (Walsham, 2012). As IS research continues to evolve to include a wider range of settings, objectives, and methodologies, it must also continue to seek involvement and contributions from other disciplines—namely those to which we have historically looked to for theoretical and methodological foundations. The challenge to achieve meaningful research contributions is increasingly complex and requires that we remain steadfastly attuned to shifts that are occurring across the greater IS research field and in its relationships with other disciplines.

Empirical investigation of phenomena without meaningful and valid measurements of the salient constructs is not probative. Focusing attention on developing ways to measure security related behaviors will be a particularly fruitful avenue for future research. Many of the issues identified in this paper are complicated by gaining access to and the proper measurement of actual security-related behaviors. As research questions are answered in each of these areas, it will be necessary for researchers to utilize tools that are not necessarily the easiest to implement, but those that are the most appropriate to address the research question of interest. We must be open to multiple methodologies—extending beyond the traditional reliance on a positivistic paradigm—thereby facilitating the discovery of theories germane to the Behavioral InfoSec research community.

This inventory of research topics and future research directions within this nomologic net is neither comprehensive nor complete. Researchers face many challenges in investigating the important phenomena within this domain, and the focus will undoubtedly change as new threats surface and technologies emerge. The scholarly community must not be myopic—scientists must constantly seek the best methods for pursuing the important research topics as they unfold.

Table 1 – Future information security themes.

Theme	We need to …	We must overcome …
Insider deviant behavior	• Differentiate insider deviant behavior from insider misbehavior and oversight • Measure deviant behaviors	• Survey approach limitations • Social desirability bias
Unmasking the mystery of the hacker world	• Clearly differentiate what type of hacker is being investigated • Understand characteristics of different types hackers • Determine the motivations of different types of hackers	• Obstacle to identification and access to hacker communities • Limited research methodologies
Improving information security compliance	• Understand appropriate context and alignment of fear-based persuasive communications with audience interests • Determine when fear is inappropriate and will backfire • Differentiate between fear as an emotion versus fear as a cognition • Utilize established behavioral modifiers, such as deterrence and perceived organizational justice • Understand the motivators of what encourages employees to be accountable and compliant • Understand how to better turn organizational insiders into security allies, as opposed to merely being security risks	• Non-uniform influence of persuasive communications • Limited methods for capturing and distinguishing the “fear” emotion
Cross-cultural InfoSec research	• Apply established cross-cultural concepts to Behavioral InfoSec research projects • Develop theoretical understandings for differences in information security behaviors from a cultural perspective	• Relying on national generalizations of culture, rather than measuring them on the individual level • A generalization of single cultural studies to cross-cultural and other cultural contexts
Data collection and measurement issues	• Improve methods for collecting and measuring security related data • Capture actual behavior (e.g., security violations, hacking, cracking, non-compliance with policies) • Better utilize non-security related data to predict security based outcomes	• Limited access to security-related data • Limited methods for capturing behavior • An under-utilization of qualitative data sources

Tackling the challenges of Behavioral InfoSec research has practical ramifications as well that extend beyond just the interests of the research community. First, as the security behaviors of individuals are understood, steps can be taken to improve their positive security behaviors while decreasing their negative security behaviors. Further, Behavioral InfoSec research may also provide insight into the design and implementation of security subsystems. According to Kuechler and Vaishnavi (2012), the design of new technology artifacts includes tacitly embedding existing theories from a number of research domains into the development of a new piece of technology. As new factors relating to individuals securing their information assets come to light, so too will opportunities for creating or enhancing new information security tools.

REFERENCES

Acquisti A, Grossklags J. Privacy attitudes and privacy behavior. Economics of Information Security 2004:165–78.

Ajzen I. Attitudes, personality and behavior. New York, NY: Open Univ Press; 2005.

Anderson B, Hansen J, Vance A, Kirwan B, Eargle D, Hinkle LJ, et al. Neural correlates of gender differences in distinguishing malware warnings and legitimate websites: a NeuroIS study. The Dewald Roode Information Security Workshop. Provo, UT, USA. IFIP WG 8.11/11.13; 2012.

Anderson CL, Agarwal R. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly 2010;34(3): 613–43.

Ayuso PN, Gasca RM, Lefevre LFT-FW. A cluster-based fault-tolerant architecture for stateful firewalls. Computers & Security 2012;31(4):524–39.

Baker W, Goudie M, Hutton A, Hylender C, Niemantsverdriet J, Novak C, et al. Verizon 2010 data breach investigations report, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf; 2010.

Barber R. Hackers profiled – who are they and what are their motivations? Computer Fraud & Security 2001;2001(2):14–7.

Bossler AM, Burruss GW. The general theory of crime and computer hacking: low self-control hackers? In: Holt TJ, Schell BH, editors. Corporate hacking and technology-driven crime: social dynamics and implications. Hershey: Information Science Reference; 2011. p. 38–67.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 2010;34(3): 523–48.

Choo K-KR. The cyber threat landscape: challenges and future research directions. Computers & Security 2011;30(8):719–31.

Cohen LE, Felson M. Social change and crime rate trends: a routine activity approach. American Sociological Review 1979;44(4):588–608.

Crossler RE. Protection motivation theory: understanding determinants to backing up personal data. 43rd Annual Hawaii International Conference on System Sciences (HICSS). Kaua'i, Hawaii, USA; 2010.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 2009;20(1):79–98.

D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 2011;20(6): 643–58.

D'Arcy J, Hovav A. Deterring internal information systems misuse. Communications of the ACM 2007;50(10):113–7.

Dimoka A. What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. MIS Quarterly 2010;34(2):373–96.

Dimoka A. How to conduct a functional magnetic resonance (fMRI) study in social science research. MIS Quarterly 2012; 36(3):811–40.

Dimoka A, Banker RD, Benbasat I, Davis FD, Dennis AR, Gefen D, et al. On the use of neurophysiological tools in information systems research: developing a research agenda for NeuroIS. MIS Quarterly 2012;36(3):679–702.

Dlamini MT, Eloff JHP, Eloff MM. Information security: the moving target. Computers & Security 2009;28(3–4):189–98.

Douglas M. Risk and blame: essays in cultural theory. New York: Routledge; 1992.

Eisenhardt KM, Graebner ME. Theory building from cases: opportunities and challenges. The Academy of Management Journal Archive 2007;50(1):25–32.

Fagnot IJ. Behavioral information security. In: Janczewski LJ, Colarik AM, editors. Encyclopedia of cyber warfare and cyber terrorism. Hershey, PA: USA: Information Science Reference; 2008. p. 199–205.

Glaser BG, Strauss AL. The discovery of grounded theory: strategies of qualitative research. London: Wledenfeld and Nicholson; 1967.

Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems 2011;28(2):203–36.

Halbert D. Discourses of danger and the computer hacker. The Information Society 1997;13(4):361–74.

Hansen JV, Lowry PB, Meservy R, McDonald D. Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems 2007;43(4):1362–74.

Herath T, Rao H. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems 2009a;47(2):154–65.

Herath T, Rao H. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 2009b;18(2):106–25.

Ho SM, McDonald N, Warkentin M. Lie to me: gender deception and detection in computer-mediated communications. The Dewald Roode Information Security Workshop. Provo, UT, USA. IFIP WG 8.11/11.13; 2012.

Hofstede G. Culture's consequences: comparing values, behaviors, institutions, and organizations across nations. 2nd ed. Sage Publications, Inc; 2001.

Hollinger RC. Hackers: computer heroes or electronic highwaymen? ACM SIGCAS Computers and Society 1991;21(1):6–17.

Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the role of top management and organizational culture. Decision Sciences 2012;43(4):615–60.

Hu Q, Xu Z, Dinev T, Ling H. Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM 2011a;54(6):54–60.

Hu Q, Zhang C, Xu Z. How can you tell a hacker from a geek? Ask whether he spends more time on computer games than sports!. The Dewald Roode Information Security Workshop. Blacksburg, VA, USA. IFIP WG 8.11/11.13; 2011b.

Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security 2012;31(1):83–95.

Jensen ML, Lowry PB, Burgoon JK, Nunamaker JF. Technology dominance in complex decision making: the case of aided credibility assessment. Journal of Management Information Systems 2010;27(1):175–202.
Jensen ML, Lowry PB, Jenkins JL. Effects of automated and participative decision support in computer-aided credibility assessment. Journal of Management Information Systems 2011;28(1):201–34.
Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Quarterly 2010;34(3): 549–66.
Kim SS, Malhotra NK. A longitudinal model of continued IS use: an integrative view of four mechanisms underlying postadoption phenomena. Management Science 2005;51(5): 741–55.
Kuechler W, Vaishnavi V. A framework for theory development in design science research: multiple perspectives. Journal of the Association for Information Systems 2012;13(6):395–423.
Leach J. Improving user security behaviour. Computers & Security 2003;22(8):685–92.
Lee SM, Lee SG, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 2004;41(6):707–18.
Lee Y. Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. Decision Support Systems 2011;50(2):361–9.
Lee Y, Larsen KR. Threat or coping appraisal: determinants of SMB executive's decision to adopt anti-malware software. European Journal of Information Systems 2009;18(2): 177–87.
Levine TR, Asada KJK, Lindsey LLM. The relative impact of violation type and lie severity on judgments of message deceitfulness. Communication Research Reports 2003;20(3): 208–18.
Levy S. Hackers: heroes of the computer revolution. New York, NY: Penguin Books; 2001.
Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. Journal of the Association for Information Systems 2010;11(7):394–413.
Lowry PB, Cao J, Everard A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures. Journal of Management Information Systems 2011;27(4): 165–204.
Lowry PB, Zhang D, Zhou L, Fu X. Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. Information Systems Journal 2010;20(3):297–315.
Mahmood MA, Siponen M, Straub D, Rao HR, Raghu T. Moving toward black hat research in information systems security: an editorial introduction to the special issue. MIS Quarterly 2010; 34(3):431–3.
McCornack SA. Information manipulation theory. Communication Monographs 1992;59(1):1–16.
McCornack SA, Levine TR, Solowczuk KA, Torres HI, Campbell DM. When the alteration of information is viewed as deception: an empirical test of information manipulation theory. Communication Monographs 1992;59(1):17–29.
Myers MD, Newman M. The qualitative interview in IS research: examining the craft. Information and Organization 2007;17(1): 2–26.
Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A. What levels of moral reasoning and values explain adherence to information security rules an empirical study. European Journal of Information Systems 2009;18(2):126–39.
Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. Computers & Security 2012;31(4): 418–36.
Ormond D, Warkentin M. Message quality and quantity manipulations and their effects on perceived risk. In: Proceedings of the national decision sciences institute (DSI) annual conference San Francisco; 2012.
Pogarsky G. Projected offending and contemporaneous rule-violation: implications for heterotypic continuity. Criminology 2004;42(1):111–36.
Posey C, Bennett R, Roberts TL, Lowry PB. When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. Journal of Information System Security 2011a;7(1):24–47.
Posey C, Bennett RJ, Roberts TL. Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. Computers & Security 2011b;30(6–7):486–97.
Posey C, Lowry PB, Roberts TL, Ellis S. The culture-influenced online community self-disclosure model: the case of working professionals in France and the UK who use online communities. European Journal of Information Systems 2010;19(2):181–95.
Posey C, Roberts TL, Lowry PB. Motivating the insider to protect organizational information assets: evidence from protection motivation theory and rival explanations. The Dewald Roode Information Security Workshop. Blacksburg, VA, USA. IFIP WG 8.11/11.13; 2011c.
Richardson R. 2010/2011 CSI computer crime and security survey, http://www.GoCSI.com; 2011.
Roberts CC. Plan-based simulation of malicious intruders on a computer system. Masters Thesis. Monteray, CA: Naval Postgraduate School; 1995.
Rogers M, Smoak ND, Liu J. Self-reported deviant computer behavior: a big-5, moral choice, and manipulative exploitive behavior analysis. Deviant Behavior 2006a;27(3):245–68.
Rogers MK, Seigfried K, Tidke K. Self-reported computer criminal behavior: a psychological analysis. Digital Investigation 2006b; 3(Suppl.):116–20.
Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty RE, editors. Social psychophysiology: a sourcebook. New York, NY, USA: Guilford; 1983. p. 153–76.
Sasse MA, Brostoff S, Weirich D. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal 2001;19(3): 122–31.
Schell BH, Dodge JL, Moutsatsos SS. The hacking of America: who's doing it, why, and how. Quorum Books; 2002.
Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly 2010;34(3):487–502.
Siponen M, Willison R. A critical assessment of IS security research between 1990–2004. In: 15th European conference on information systems. St. Gallen, Switzerland; 2007. p. 1551–9.
Siponen M, Willison R. Information security management standards: problems and solutions. Information & Management 2009;46(5):267–70.
Srite M, Karahanna E. The role of espoused national cultural values in technology acceptance. MIS Quarterly 2006;30(3): 679–704.
Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Computers & Security 2005;24(2):124–33.
Stanton JM, Stam KR, Mastrangelo PM, Jolton JA. Behavioral information security: an overview, results, and research agenda. In: Zhang P, Galletta DF, editors. Human–computer interaction and management information systems: foundations. Armonk, NY, USA: M.E. Sharpe; 2006. p. 262–80.
Straub D, Limayem M, Karahanna-Evaristo E. Measuring system usage: implications for IS theory testing. Management Science 1995;41(8):1328–42.

Straub DW. Black hat, white hat studies in information security. Keynote Presentation of the 1st IFIP 8.2 Security Conference. Cape Town, South Africa; 2009.
Straub DW, Nance WD. Discovering and disciplining computer abuse in organization. MIS Quarterly 1990;14(1):45.
Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Quarterly 1998; 22(4):441–69.
Taylor P. Hackers: crime in the digital sublime. London: Routledge; 1999.
Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E. The insider threat to information systems and the effectiveness of ISO17799. Computers & Security 2005;24(6):472–84.
Vance A, Molyneux B, Lowry PB. A new approach to the problem of unauthorized access: raising perceptions of accountability through user interface design features. The Dewald Roode Information Security Workshop. Blacksburg, VA, USA. IFIP WG 8.11/11.13; 2011.
Vance A, Molyneux B, Lowry PB. Reducing unauthorized access by insiders through end-user design: making users accountable. In: 45th Annual Hawaii international conference on system sciences (HICSS). Maui, Hawaii, USA; 2012a.
Vance A, Ouimet K, Eargle D. Enhancing password security through interactive fear appeals. The Dewald Roode Information Security Workshop. Provo, UT, USA. IFIP WG 8.11/ 11.13; 2012b.
Venkatesh V, Davis FD. A theoretical extension of the technology acceptance model: four longitudinal field studies. Management Science 2000;46(2):186–204.
Vroom C, von Solms R. Towards information security behavioural compliance. Computers & Security 2004;23(3):191–8.
Walsham G. Are we making a better world with ICTs? Reflections on a future agenda for the IS field. Journal of Information Technology 2012;27(2):87–93.
Warkentin M, Johnston AC, Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems 2011a;20(3):267–84.
Warkentin M, Shropshire J, Johnston AC. Security software discontinuance. 2006 Workshop on Information Security and Assurance. Milwaukee, WI; 2006.
Warkentin M, Straub D, Malimage K. Measuring the dependent variable for research into secure behaviors. Decision Sciences Institute Annual National Conference. Boston, MA; 2011b.
Warkentin M, Straub D, Malimage K. Measuring secure behavior: a research commentary. In: Proceedings of the annual symposium on information assurance. Albany, New York; 2012a.
Warkentin M, Walden EA, Johnston AC, Straub DW. Identifying the neural correlates of protection motivation for secure IT behaviors. Gmunden Retreat on NeuroIS 2012b;2012. Gmunden, Austria.
Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems 2009;18(2):101–5.
Wikström PO. Crime as alternative: towards a cross-level situational action theory of crime causation. In: McCord J, editor. Beyond empiricism: institutions and intentions in the study of crime. New Brunswick, NJ: Transaction Publishers; 2004. p. 1–38.
Wikström PO. Linking individual, setting, and acts of crime. situational mechanisms and the explanation of crime. In: Wikström H, Sampson RJ, editors. The explanation of crime: contexts, mechanisms, and development. Cambridge, UK: Cambridge University Press; 2006.
Willison R. Understanding the perpetration of employee computer crime in the organisational context. Information and Organization 2006;16(4):304–24.
Willison R, Backhouse J. Opportunities for computer crime: considering systems risk from a criminological perspective. European Journal of Information Systems 2006;15(4): 403–14.
Willison R, Warkentin M. Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly; 2013;37(1).
Woon IMY, Tan GW, Low RT. A protection motivation theory approach to home wireless security. In: Twenty-sixth international conference on information systems (ICIS); 2005. p. 367–80.
Wright RT, Marett K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. Journal of Management Information Systems 2010;27(1):273–303.
Yar M. Computer hacking: just another case of juvenile delinquency? The Howard Journal of Criminal Justice 2005; 44(4):387–99.
Yin RK. Case study research: design and methods. Newbury Park, CA: Sage Publications; 2009.
Young R, Zhang L, Prybutok VR. Hacking into the minds of hackers. Information Systems Management 2007;24(4):281–7.
Zafar H, Clark JG. Current state of information security research in IS. Communications of the Association for Information Systems 2009;24(34):557–96.
Zhang D, Lowry PB. Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems. Journal of Global Information Management 2008;16(1):61–92.
Zhang D, Lowry PB, Zhou L, Fu X. The impact of individualism-collectivism, social presence, and group diversity on group decision making under majority influence. Journal of Management Information Systems 2007;23(4):53–80.
Zhi-jun W, Hai-tao Z, Ming-hua W, Bao-song P. MSABMS-based approach of detecting LDoS attack. Computers & Security 2012;31(4):402–17.

Dr. Robert E. Crossler is an Assistant Professor in the Management and Information Systems department at Mississippi State University. He received his Ph.D. in Information Systems from Virginia Tech. His research focuses on the factors that affect the security and privacy decisions that individuals make. He has several publications in the IS field, including such outlets as *MIS Quarterly*, *Decision Support Systems*, *Journal of Information Systems Security*, *Americas Conference on Information Systems*, *The Annual Conference of the Decision Sciences Institute*, and *Hawaii International Conference on System Sciences*.

Dr. Allen C. Johnston is an Assistant Professor in the School of Business at the University of Alabama at Birmingham. He received his Ph.D. in Information Systems from Mississippi State University. His works can be found in such outlets as *MIS Quarterly*, *European Journal of Information Systems*, *Communications of the ACM*, and *DATA BASE for Advances in Information Systems*. The primary focus of his research has been in the area of information assurance and computer security, with a specific concentration on the behavioral aspects of information security and privacy.

Dr. Paul Benjamin Lowry is an Associate Professor of Information Systems at the Department of Information Systems of the City University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona. His works have been published in such outlets as *MIS Quarterly*; *Journal of Management Information Systems*; *Journal of the Association for Information Systems*; *Information Systems Journal*; *European Journal of Information Systems*; and others. Dr. Lowry's research interests include behavioral security issues, HCI, E-commerce and supply chains, and Scientometrics.

Dr. Qing Hu is the Chair and Union Pacific Professor in Information Systems in the Department of Supply Chain and Information Systems at Iowa State University. He received his Ph.D. in Computer Information Systems from the University of Miami, Florida. His work has appeared in some of the top journals in the information systems discipline such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *California Management Review*, and *Communications of the ACM*. His research interests include strategic IT management, IT value, information security, and cross culture issues in information technology.

Dr. Merrill Warkentin is a Professor of MIS and the John and Carole Ferguson Notable Scholar in the College of Business at Mississippi State University. He earned his Ph.D. from the University of Nebraska-Lincoln. His research has appeared in such journals as *MIS Quarterly*, *Decision Sciences*, *European Journal of Information Systems*, *Decision Support Systems*, *Communications of the ACM*, and *Information Systems Journal*. He is the AIS Departmental Editor for IS Security & Privacy, and the next chair of the IFIP Working Group on Information Systems Security Research. His primary research focus is in behavioral IS security issues.

Dr. Richard Baskerville is Board of Advisors Professor in the Department of Computer Information Systems, J. Mack Robinson College of Business at Georgia State University. His research specializes in security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. He is co-editor of the *European Journal of Information Systems*. He is chair of the International Federation for Information Processing Working Group on Information Systems Security Research. Baskerville holds degrees from the University of Maryland, and the London School of Economics.