Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Identification of Behavioral Factors within Organizations that Can Improve Information Systems Security Compliance

CAPSTONE REPORT

Matthew Peterson
Faculty Research Assistant
Oregon State University
Center for Genome Research
And Biocomputing

University of Oregon
Applied Information
Management
Program

May 2014

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Lecturer, AIM Program

Identification of Behavioral Factors within Organizations that Can Improve Information Systems Security Compliance

Matthew Peterson

Oregon State University

Center for Genome Research and Biocomputing

Abstract

Organizational information assets require protection and cannot be secured by technological means alone. This annotated bibliography, reviewing literature from 2004 to 2014, identifies the employee behavioral factors on which managers should focus to improve information systems security policy (ISSP) compliance within their organizations. The categories of biases, beliefs, perceptions, and motivations are discussed. Specific recommendations for managers include addressing human error, attitudes, social context, self-efficacy, and extrinsic motivations.

Keywords: information systems security policy, information security, compliance, behavioral factors, human factors, human error, motivation

Table of Contents

List of Tables and Figures

Introduction to the Annotated Bibliography

Problem

Information is considered a valuable asset to organizations and thus requires protection, which is enacted through management and governance plans (Herath & Rao, 2009; Thomson & von Solms, 2005). Information assets, knowledge assets, and information capital all provide value to organizations (Berzkalne, & Zelgalve, 2014; Glazer, 1991; Kakabadse, Kouzmin, & Kakabadse, 2001;Wiig, 1997). The amount of value that these assets provide is considered significant, although the value may be difficult to quantify; developing accurate measures and accounting of such value is an evolving field of research (Bontis, 2001; Wilson & Stenson, 2008).

Organizational failures to secure information assets can result in a variety of negative outcomes. For example, a survey conducted by the Ponemon Institute, LLC (2013) reports that security breaches, such as disclosure of protected personal data, can cost companies millions of dollars. A company's market value may be significantly impacted from the public announcements of security breaches (Acquisti, Friedman, & Telang, 2006; Campbell, Gordon, Loeb, & Zhou, 2003; Goel & Shawky, 2009). Response costs, such as labor costs, to identify, eliminate, and recover from security breaches can also be incurred (Lee, Fan, Miller, Stolfo, & Zadok, 2002).

Kruger and Kearney (2006) define information security as the focus "on protecting the confidentiality, integrity and availability of information" (p. 289). Herath and Rao (2009) point out that "information security cannot be achieved through only technological tools" and that "empirical research on end-user security behaviors and factors … is still in its infancy" (p.154). Focusing on end-user behaviors, e.g., human factors, is important as they are considered the

"weakest link" in information security (Huang, Rau, & Salvendy, 2007; Ifinedo, 2014; Warkentin & Willison, 2009). Examples of human factors that may influence ISSP compliance include biases in the areas of estimation and unrealistic optimism (Lichtenstein, Slovic, Fischhoff, Layman, & Combs, 1978; Weinstein, 1987). In addition, individuals who encounter novel situations may experience difficulty when making decisions that involve risk (Fischhoff, 2002). These individuals may only rely on overly simplified responses and heuristics or "rules of thumb" (Fischhoff, 2002, p. 52). A survey conducted by the Ponemon Institute, LLC (2013) demonstrated that at least 35% of security breaches concerned human error.

Purpose

The purpose of this annotated bibliography is to identify behavioral factors within organizations that can improve information systems security compliance (ISSP), defined by Ifinedo (2012) as a "mechanism for shaping or influencing the behaviors of their employees with respect to how organizational IS resource [*sic*] are used" (p. 84). Sources that identify the human factors that directly affect compliance, such as human error, the ability to perceive risk, and the rewarding of positive behavior are examined (Australian Government, Department of Defence, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organization, 2010). The effectiveness of intrinsic and extrinsic motivations as they relate to human factors with regards to ISSP compliance is also evaluated (Herath & Rao, 2009; Ruighaver, Maynard, & Chang, 2007; Son, 2011). Finally, sources are included that focus on the specific case of agency literature as applied to ISSP compliance using incentive and disincentive mechanisms (Herath & Rao, 2009), as well as literature that explores the larger context of *agency relationships*, defined by Herath and Rao (2009) as "whenever one party (principal) entrusts some decision making authority to another party (agent)" (p. 155).

However, technical implementation of industry and government information security policies and standards is not addressed (Höne & Eloff, 2002). Moreover, the problem does not focus on improving ISSP compliance for employees with malicious intent or ethical issues.

Audience

Rather than placing the onus of ISSP compliance on IT professionals, e.g., the Chief Security Officer, several authors target general management as being responsible for fostering and supporting a security culture. Ruighaver, Maynard, and Chang (2007) state that "security culture cannot be carried out in isolation of wider organizational culture," in which managers are directly involved (p. 56). In addition, security processes can be impacted by daily, non-IT operations, requiring managers to be directly involved as stakeholders to ensure their success (Ruighaver, Maynard, & Chang, 2007). Ifinedo (2014) suggests "influential people in organisations who are capable of motivating or shaping the opinions of others could be tasked to champion the cause of ISSP compliance" (p.76). Pahnila, Siponen, and Mahmood (2007) find in their study that "positive social pressure (normative belief) towards IS security policy compliance from top management … is important for ensuring employees' IS security policy compliance" (p.7).

The target audience for this annotated bibliography is therefore organizational managers. Managers benefit from this annotated bibliography by learning techniques for improving ISSP compliance in behavioral and social contexts. In addition, managers explore literature that describes the lack of success that traditional methods, e.g., sanctions and penalties, may have on compliance (Ifinedo, 2014).

Research Questions

Main question. On which employee behavioral factors should managers focus within their organizations to improve information security compliance?

Sub-question. How do behavioral factors influence employee behavior with regards to information security compliance?

Search Strategy

The University of Oregon Libraries' OneSearch is used after connecting via the Cisco AnyConnect Secure Mobility Client. Initial searches use the terms *information security* and *self-efficacy* against the default subject "General/Interdisciplinary," i.e., the databases "Academic Search Premier," "JSTOR," "Project Muse," and "Web of Science." The results of these initial searches and suggested articles via the Elsevier ScienceDirect website helped refine the burning question and its subsequent search terms. Google Scholar is used repeatedly to confirm that relevant articles obtained through OneSearch and individual, off-site databases, are not missed.

Databases. The following databases are used via OneSearch and external to the UO Library site:

- Academic Search Premier
- ACM Digital Library
- ArSXiv.org
- Computer Source
- Google Scholar
- IEEE Computer Science Digital Library
- IEEE Xplore Digital Library
- JSTOR
- Project Muse

- ProQuest (and its sub-databases)
- ScienceDirect
- UO Local Catalog
- Web of Science

OneSearch databases in the following subject categories are also used but predominately duplicated the results found on the above databases:

- Business
- Psychology
- Social Sciences
- Sociology

Terms. A thorough search yields the following list of terms; subsequent searches combine these search terms in a variety of ways:

- information security
- information security policy
- information security awareness
- compliance
- self-efficacy
- behavior/behavioral (behaviour/behavioural)
- motivation
- culture/cultural
- social/socialization
- relationships
- human factors

- organizational
- governance

Documentation Approach

Qualitative researchers should first focus on "establishing the protocol for recording information" before beginning their data recording procedures (Creswell, 2009, p. 181). The Zotero Standalone for Mac software package is chosen given its ability to "assist in writing papers, managing references, and organizing research materials" (Roy Rosenzweig Center for History and New Media, 2014a, 2014f; Vanhecke, 2008). Each reference is added to Zotero using the "Add Item(s) by Identifier" button and entering the journal article's Digital Object Identifier, if available (Digital Object Identifier System, 2014; Roy Rosenzweig Center for History and New Media, 2014b). The majority of journal articles added did not automatically populate the abstract field metadata, so this information is manually added. Additional metadata, such as search terms, article focus, and relevancy are tracked using Zotero's notes feature (Roy Rosenzweig Center for History and New Media, 2014e). PDF copies of journal articles, if available, are also uploaded into Zotero using the "Attach Stored Copy of File..." feature (Roy Rosenzweig Center for History and New Media, 2014c). Finally, journal articles are further sorted using the collection and subcollection feature to help classify the focus of each article to determine whether inclusion in the annotated bibliography and/or references is warranted (Roy Rosenzweig Center for History and New Media, 2014d).

Reference Evaluation Criteria

The credibility of each reference is evaluated before selection using Bell and Frantz's (2013) five areas: authority, objectivity, quality, currency, and relevancy. References are considered authoritative if they appear in either peer-reviewed journals or recognized conference

proceedings and the author is affiliated with a reputable institution (Bell & Frantz, 2013). Objectivity is evaluated by examining the author's stated purpose, potential biases, acknowledgement of any biases, and whether the author's conclusions are supported by evidence (Bell & Frantz, 2013). A high-quality reference is identified if the reference is clearly written and well organized—usually criteria for publication in peer-reviewed journals (Bell & Frantz, 2013). While numerous short magazine articles are found, e.g., via the "IEEE Computer Science Digital Library," the results are not included as part of the reference material due to their lack of depth and possible lack of peer review. Currency is evaluated by sourcing articles within the last 10 years, which demarcates the popularization of Web 2.0, beginning in 2004 (Lawton, 2007; O'Reilly, 2007). Reference materials appearing in the annotated bibliography may exceed the 10-year time frame, especially in the fields of psychology and sociology, if they still are relevant to the research. Relevance is evaluated for each reference primarily based upon its source, such as peer-reviewed journals or popular press. In addition, the relevance of each source is examined for inclusion, and both primary sources representing research studies and secondary sources analyzing phenomena are included (Bell & Frantz, 2013).

Annotated Bibliography

The following Annotated Bibliography presents 15 references that examine employee behavioral factors and their influence on ISSP compliance. These references help managers determine on which behavioral factors they should focus to improve information security compliance within their organizations. Each annotation consists of the full bibliographic citation, the full abstract, and a summary. The summaries represent the research findings and conclusions of the articles' authors. Each summary discusses the behavioral factors that may influence ISSP compliance; these behavioral factors are primarily from psychology and sociology research areas. The ultimate goal of the summaries is to provide managers with insight as to where they can best focus their efforts to increase ISSP compliance.

Australian Government, Department of Defence, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organization. (2010). *Human factors and information security: Individual, culture and security environment*. (DSTO-TR-2484). Retrieved from http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10094/1/DSTO-TR-2484%20PR.pdf

Abstract. The application of information security technologies do not always result in improved security. Human factors play a significant role in computer security; factors such as individual difference, cognitive abilities and personality traits can impact on behaviour. Information security behaviours are also greatly influenced by an individual's perception of risk. All of these factors are also affected by the organisation culture and security environment in which they occur. These factors interact with one another and

can result in behaviours that are often detrimental to information security. This report provides recommendations as to how these human and cultural factors can be influenced to result in more positive behaviours and lead to more secure information environments.

Summary. This article summarizes several human factors relating to risk perception and cognitive biases and discusses their potential impact on ISSP compliance:

- Availability heuristic – the inaccurate estimation of an event's likelihood and importance based upon ease of recall (Slovic, Fischhoff, & Lichtenstein, 1979; Tversky & Kahneman, 1973). Chronic, common risks, such as poorly documented ISSP procedures, are likely underestimated, while dramatic events like hacking are likely overestimated.
- Optimism bias – the belief that the risk for negative outcomes is greater for others than for themselves (Sjöberg, 2000). For example, users may believe they would never be potential targets of hackers (McIlwraith, 2006). The bias can be compounded if users do not receive feedback or warnings that their insecure behaviors are creating further risk (Weinstein, 1987).
- Level of control – the belief that threats are less risky in situations where individuals feel that they have control over their environment (Kreuter & Strecher, 1995; Slovic, Fischhoff, & Lichtenstein, 1978). Individuals who are overly optimistic may overestimate their control and subsequently take more risks.
- Level of knowledge – lack of understanding about a topic can impact an individual's perception of risk and their subsequent decisions (Fischhoff, 2002). This lack of knowledge of security may lead to inappropriate or ineffective decisions (Lacohée, Phippen, & Furnell, 2006).

- Risk homeostasis – Individuals will change their behaviors to compensate for changing levels of perceived risk (Wilde, 2001). Incomplete understanding of a new security situation and its associated risks may result in increased risk-taking behaviors (Stewart, 2004).
- Cumulative risk – Small security risks taken by individuals can accumulate into a larger, additive risk over time (Fischhoff, 2002). It is shown that individuals have a poor understanding of cumulative risk and thus may continue small risk-taking behaviors (Slovic, 2000).
- Omission bias – Failure to perform a correct action is perceived to be less of an issue than committing an incorrect action (Ritov & Baron, 1992). For example, individuals may perceive the omission of not regularly changing their password to be a less significant violation of ISSP than writing their password down.
- Influence of framing – The likelihood of an individual taking a risk increases when possible losses are presented; conversely, risk-taking behaviors decrease when possible gains are communicated (Kahneman & Tversky, 1979). Focusing on the communication of gains in security, as opposed to losses, may increase ISSP compliance.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=52546353&site=ehost-live&scope=site

Abstract. Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security. Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, under- standing compliance behavior is crucial for organizations that want to leverage their human capital. This research identifies the antecedents of employee compliance with the information security policy (ISP) of an organization. Specifically, we investigate the rationality-based factors that drive an employee to comply with requirements of the ISP with regard to protecting the organization's information and technology resources. Drawing on the theory of planned behavior, we posit that, along with normative belief and self-efficacy, an employee's attitude toward compliance determines intention to comply with the ISP. As a key contribution, we posit that an employee's attitude is influenced by benefit of compliance, cost of compliance, and cost of noncompliance, which are beliefs about the overall assessment of consequences of compliance or noncompliance. We then postulate that these beliefs are shaped by the employee's outcome beliefs concerning the events that follow compliance or noncompliance: benefit of compliance is shaped by intrinsic benefit, safety of resources, and rewards, while cost of compliance is shaped by work impediment; and cost of noncompliance is shaped by intrinsic cost, vulnerability of resources, and sanctions. We also investigate the impact of information security awareness (ISA) on outcome beliefs and an employee's attitude toward compliance with the ISP. Our results show that an employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. Outcome beliefs significantly affect

beliefs about overall assessment of consequences, and they, in turn, significantly affect an employee's attitude. Furthermore, ISA positively affects both attitude and outcome beliefs. As the importance of employees' following their organizations' information security rules and regulations increases, our study sheds light on the role of ISA and compliance-related beliefs in an organization's efforts to encourage compliance.

Summary. The authors of this article survey 464 employees from diverse organizations to examine how beliefs and attitudes towards ISSP compliance and their potential outcomes influence one other. The theory of planned behavior (TPB) is used to develop hypotheses testing individuals' intention to comply with ISSP requirements by examining three areas (Ajzen, 1991): (1) *behavioral beliefs* based upon participants' positive values assigned to compliance, (2) *normative beliefs* regarding the perceptions of social pressure from peers and managers to comply, and (3) *perceived behavioral control* as an extension of *self-efficacy theory* that addresses participants' beliefs in their abilities to achieve compliance (Bandura, 1977). Relational choice theory (RCT) is used to develop three hypotheses that test what participants assess as the: (1) benefits of ISSP compliance as they relate to favorable consequences, (2) costs of compliance as "overall expected unfavorable consequences," and (3) costs of noncompliance as "overall expected unfavorable consequences." In addition, the three RCT hypotheses contain numerous sub-hypotheses that address outcome beliefs, including intrinsic benefit, safety of resources, rewards, work impediment, intrinsic cost, vulnerability of resources, and sanctions. Using a component-based partial least squares analysis, the authors conclude that the independent variables of *attitude towards compliance*, *normative beliefs*, *self-efficacy*, *benefits of compliance*, *costs of compliance*, and *costs of noncompliance* are

statistically significant factors influencing the dependent variable of *intention to comply* with ISSP ($p < 0.01$).

Guo, K. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32, 242-251. doi: 10.1016/j.cose.2012.10.003 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404812001666

Abstract. Security-related behavior in the workplace has recently drawn much attention from scholars in the information systems literature. Many studies, however, have reported inconsistent and sometimes contradictory results about the effects of some key factors such as sanctions. We argue that one of the reasons causing the inconsistent findings is the divergent conceptualizations of security-related behavior. In this paper, we conducted an extensive review of the divergent concepts. Many of the concepts overlap with each other on some dimensions and yet are different on others. By delineating and synthesizing the differences, we proposed a framework for conceptualizing security-related behavior. The framework can facilitate the development of consistent and comparable terms and concepts in future studies. Implications for research are also discussed.

Summary. Security-related behaviors as described in the IS literature are first classified into seven dimensions: (1) *intentionality* as intentional or non-intentional, e.g., misuse and human error; (2) *motive* as malicious or non-malicious; (3) *expertise* to perform a behavior; (4) *job relatedness* as it applies to a behavior; (5) *consequence* of the behavior, such as increasing risk or incurring damage; (6) *action vs. inaction*, such as policy

compliance or omission; and (7) *rule* violation of both laws and organizational policy. With respect to these dimensions, the authors examine several conceptualizations of security-related behaviors from the current IS literature: computer abuses/security contravention, unethical use, omissive security behavior, IS misuse, violation of policy, non-malicious security violation, information security policy abuse, and security policy compliance. The review finds "contradictory conclusions were obtained from the same theoretical perspective" in the IS literature (Guo, 2013, p. 246). The author further attempts to clarify these contradictions and concludes, "many differences exist between desirable and undesirable behaviors" (Guo, 2013, p. 248). Based upon this literature review, the author proposes a conceptual framework for classifying security-related behaviors along the previously defined seven dimensions into four categories: security assurance behavior (SAB), security compliant behavior (SCB), security risk-taking behavior (SRB), and security damaging behavior (SDB).

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. doi: 10.1016/j.im.2012.08.001 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720612000584

Abstract. We proposed and empirically tested a mediating model for examining the effects of multilevel sanctions on preventing information security violations in the workplace. The results of the experiment suggested that personal self-sanctions and workgroup sanctions have significant deterrent effects on employee security violations, but that the effect of organizational sanctions becomes insignificant when the other two

types of sanctions are taken into account. Theoretically, the study pointed out the importance of personal self-sanctions and informal workgroup sanctions. Practically, our results suggested that an "influencing" strategy may be more effective than an "enforcing" one in information security management.

Summary. Based upon research by Tyler and Balder (2005), the authors classify sanctions in an organizational setting into three categories: (1) *organizational sanctions* as the threat and administration of disciplinary action, (2) *workgroup sanctions* influenced by the approval and disapproval of coworkers, and (3) *personal self-sanction* from employees who have an intrinsic desire to comply with ISSP. The authors propose a theoretical framework along with a set of hypotheses that the three sanctions negatively influence employee intentions to violate ISSP. Additional hypotheses include that the three sanctions will positively influence each other. To test these hypotheses, the authors survey a total of 335 organizational computer users via paper and web-based surveys and perform a partial least squares regression analysis. Their findings support the hypotheses that the independent variables of personal self-sanctions promoting ISSP compliance and perceived workgroup sanctions from noncompliance have significant negative influences on the dependent variable of *intentions to violate security policies* with p values < 0.05 and < 0.001, respectively, and that perceived organizational sanctions from noncompliance have no direct, significant effect. Their findings also support the hypotheses that the independent variables of perceived organizational sanctions from noncompliance and perceived workgroup sanctions from noncompliance have significant positive influences on the dependent variable of personal self-sanctions promoting ISSP compliance with p values < 0.001. Finally, the authors find that the positive influence of

the independent variable perceived organizational sanctions from noncompliance on the dependent variable of perceived workgroup sanctions from noncompliance is significant with $p < 0.001$. Participant demographics suggest that senior-level employees are more likely to commit ISSP violations than their subordinates. These findings help suggest that ISSP compliance can be improved by: (a) better educating employees so they can hold themselves accountable, (b) supporting workgroup sanctions by training role models who can act as ISSP advocates, and (c) placing less emphasis on enforcing organizational sanctions that may have little effect.

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. doi:10.1016/j.dss.2009.02.005 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167923609000530

Abstract. Secure management of information systems is crucially important in information intensive organizations. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. Thus, the area of end-user security behaviors in organizations has gained an increased attention. In information security observing end-user security behaviors is challenging. Moreover, recent studies have shown that the end users have divergent security views. The inability to monitor employee IT security behaviors and divergent views regarding security policies, in our view, provide a setting where the principal agent paradigm applies. In this paper, we develop and test a theoretical model of the incentive effects of penalties, pressures and perceived effectiveness of employee actions that enhances our

understanding of employee compliance to information security policies. Based on 312 employee responses from 77 organizations, we empirically validate and test the model. Our findings suggest that security behaviors can be influenced by both intrinsic and extrinsic motivators. Pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions. In analyzing the penalties, certainty of detection was found to be significant while surprisingly, severity of punishment was found to have a negative effect on security behavior intentions. We discuss the implications of our findings for theory and practice.

Summary. This article surveys the behavioral information security literature and identifies the theories either used or proposed by others. The authors then discuss their own theory based upon *agency theory* or *principal agent paradigm* (Eisenhardt, 1989), e.g., defined by Herath and Rao (2009a) as "whenever one party (principal) entrusts some decision making authority to another party (agent)" (p. 155). The authors propose a theoretical framework based upon the incentive mechanisms of penalties, social pressures, and perceived effectiveness. This approach includes individual hypotheses that the *severity of penalty*, *certainty of penalty*, *normative beliefs*, *peer behavior*, and *perceived effectiveness* of these incentive mechanisms are all positively associated with the intention to comply with ISSPs. To test these hypotheses, the authors survey 312 participants from 77 different organizations. To determine significance, the authors use a partial least squares regression analysis employing a component-based approach for estimation with the dependent variable of *policy compliance intention*. Their findings

support all of the hypotheses except for severity of penalty, which actually negatively affects intentions of security behavior ($p < 0.01$). In particular, penalties like dismissal may be unlikely to happen and may therefore not increase ISSP compliance intentions. Of the five hypotheses, normative beliefs (i.e., perceptions of social pressure from peers and managers to comply) is the most statistically significant in support of ISSP compliance intentions ($p < 0.001$).

Huang, D., Rau, P.P. & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. Jacko (Ed.). Human-Computer Interaction, Part IV (pp. 906-915). Heidelberg: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-73111-5_100

Abstract. Information security is a great concern to computer users, which is not only a technical problem, but also related to human factors. The objective of this study is to investigate the factors that can influence people's perception of different threats to information security. In the survey study, 602 respondents were asked to evaluate one of 21 common threats to information security with regard to its position on each of the 20 threat-related items. An exploratory factor analysis was then conducted, and a six-factor structure modeling people's perception of different threats to information security was derived. The relations between the factors and the perceived overall danger of threats were also tested by multiple regression analyses.

Summary. This article examines numerous influences of risk perception on information security. The authors perform a subsequent exploratory factor analysis and survey the IS literature to develop and organize a set of 21 common security threats into 12 categories.

Examining the existing literature on the *psychometric paradigm*, the authors develop a set of 20 influences on risk perception from a known set of 47 (Covello, 1983, 1992; Covello & Merkhofer, 1994; Fischhoff, Slovic, Lichtenstein, Read, & Cambs, 1978; Slovic, 1987, Slovic, Fischhoff, & Lichtenstein, 1980). To understand the influences of risk perception on information security, they survey 646 participants from a single organization and asked the participants to rate various influences on risk perception. Initial survey findings include the following influences having the largest impact on risk perception of information security: the *severity of consequences* of the threat is serious, *ease of reduction* of the threat's effectiveness, and wide *scope of impact* by the threat. The authors then conduct an exploratory factor analysis, grouping the 20 influences into six factors: knowledge, impact, severity, controllability, possibility, and awareness. Stepwise multiple regression analysis of survey data reveals a significant, positive effect on the dependent variable of perceived dangers of information security for four of the six factors ($p < 0.001$): knowledge, impact, severity, and possibility. Managers may use these factors to further develop ISSP with a focus on how users perceive threats and engage in secure behaviors.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. doi:10.1016/j.cose.2011.10.007 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404811001337

Abstract. This research investigated information systems security policy (ISSP) compliance by drawing upon two relevant theories i.e. the theory of planned behavior

(TPB) and the protection motivation theory (PMT). A research model that fused constituents of the aforementioned theories was proposed and validated. Relevant hypotheses were developed to test the research conceptualization. Data analysis was performed using the partial least squares (PLS) technique. Using a survey of 124 business managers and IS professionals, this study showed that factors such as self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence ISSP behavioral compliance intentions of employees. The data analysis did not support perceived severity and response cost as being predictors of ISSP behavioral compliance intentions. The study's implications for research and practice are discussed.

Summary. To better understand the behaviors involved in ISSP compliance, the author develops a research model based upon the theory of planned behavior (TPB) and the protection motivation theory (PMT) (Ajzen, 1991; Rogers, 1983). The TPB informs how the constituents of *behavior beliefs*, *subjective norms*, and *perceived behavioral controls* influence an individual's behavior (Ajzen, 1991; Bandura, 1977). The PMT informs both an individual's threat appraisal of dangerous events and coping appraisal to cope with a threat and avert any negative repercussions (Rogers, 1983). From these theories, the author derives seven main constructs that may relate to ISSP compliance behavioral intention: *subjective norms, attitude, self-efficacy, response cost, response efficacy, perceived severity*, and *perceived vulnerability*. To test whether these constructs contribute to ISSP compliance, the author conducts a survey with 124 participants, representing non-IS managers and IS professionals from a variety of organizations. To determine significance, the author uses a Partial Least Squares (PLS) analysis. Five

independent variables, namely subjective norms ($p < 0.01$), attitude ($p < 0.001$), self-efficacy ($p < 0.01$), response efficacy ($p < 0.01$), and perceived vulnerability ($p < 0.01$) increase the dependent variable of ISSP compliance behavior intentions. In contrast, the independent variable of perceived severity of sanctions decreases ISSP compliance ($p < 0.05$), and the construct of response cost does not affect ISSP compliance behavior intentions. The results of this study suggest how ISSP effectiveness can be increased through departmental ISSP advocates and by providing additional training to increase response and self-efficacy.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720613000980

Abstract. This study investigated employees' information systems security policy (ISSP) compliance behavioural intentions in organisations from the theoretical lenses of social bonding, social influence, and cognitive processing. Given that previous research on ISSP compliance has been based on deterrence theory, this study seeks to augment and diversify research on ISSP compliance through its theoretical perspective. Relevant hypotheses were developed to test the research conceptualisation. Data from a survey of business managers and IS professionals confirmed that social bonds that are formed at work largely influence attitudes towards compliance and subjective norms, with both constructs positively affecting employees' ISSP compliance. Employees' locus of control and capabilities and competence related to IS security issues also affect ISSP compliance

behavioural intentions. Overall, the constructs in the research model enhance our understanding of the social-organisational and psychological factors that might encourage or accentuate employees' ISSP compliance in the workplace.

Summary. To better understand the behaviors involved in ISSP compliance, the author develops a research model based upon the theory of planned behavior (TPB), social cognitive theory (SCT), and social bond theory (SBT) (Ajzen, 1991; Bandura, 1977; Hirschi, 2002). The TPB informs how the constituents of *behavior beliefs*, *subjective norms*, and *perceived behavioral controls* influence an individual's behavior (Ajzen, 1991; Bandura, 1977). The SCT informs how an individual learns based upon his/her environment, addressing both an individual's *locus of control* and *self-efficacy* (Bandura, 1977; Rotter, 1966; Workman, Bommer, & Straub, 2008). The SBT informs how an individual maintains social bonds with others in his/her organization and classifies these bonds as *attachment*, *commitment*, *involvement*, or *personal norms* (Hirschi, 2002). From the theories, the author derives eight main constructs that may relate to *ISSP compliance behavioral intentions*: *attachment*, *commitment*, *involvement*, *personal norms*, *subjective norms*, *attitude*, *locus of control*, and *self-efficacy*. To test whether these constructs contribute to ISSP compliance, the authors conduct a survey of 124 non-IS managers and IS professionals from a variety of organizations. To determine significance, the author uses a partial least squares analysis. The independent variables from TPB and SCT increase the dependent variable of ISSP compliance behavioral intentions, with attitude toward ISSP compliance being the most highly significant ($p < 0.001$). All bonds from SBT positively influence attitude toward ISSP compliance except for attachment, which negatively influences it ($p < 0.01$). The author suggests that "it is possible for an

employee to have a positive attitude about his or her organisation's ISSP yet hold differing perceptions from coworkers" (Ifinedo, 2014, p. 75). The SBT bonds of attachment ($p < 0.05$) and personal norms ($p < 0.01$) as independent variables positively influence the dependent variable of subjective norms, while commitment and involvement do not influence subjective norms. This study suggests that ISSP compliance can be increased by addressing it as a *social issue* and by creating delegating individuals to act as ISSP advocates. In addition, an increase in ISSP compliance may be possible through regular communication, training, and streamlining of procedures.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3), 215-228. doi: 10.1016/j.cose.2008.11.003 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808001181

Abstract. Privacy breaches and their regulatory implications have attracted corporate attention in recent times. An often overlooked cause of privacy breaches is human error. In this study, we first apply a model based on the widely accepted GEMS error typology to analyze publicly reported privacy breach incidents within the U.S. Then, based on an examination of the causes of the reported privacy breach incidents, we propose a defense-in-depth solution strategy founded on error avoidance, error interception, and error correction. Finally, we illustrate the application of the proposed strategy to managing human error in the case of the two leading causes of privacy breach incidents. This study finds that mistakes in the information processing stage constitute the most cases of

human error-related privacy breach incidents, clearly highlighting the need for effective policies and their enforcement in organizations.

Summary. This article examines organizational privacy breaches due to human error using Reason's (1990) generic error modeling system (GEMS). The GEMS defines human errors as either a *slip* by incorrectly performing a correct action or a *mistake* by correctly performing an incorrect action based upon a wrong decision. To apply the GEMS model, the authors compile and analyze a data set of 701 documented U.S. privacy breach incidents due to human error between 2005 and 2008. The authors then perform a literature review of methods to address human error in data breaches and propose a three-part error management program: (1) analysis of the top causes of breaches, which include equipment loss, Internet threats, and inappropriate skill when using IT; (2) developing a defense-in-depth error management strategy based upon *error avoidance*, *error interception*, and *error correction*; and (3) a periodic analysis of the effectiveness of the strategy during error correction. Error avoidance focuses on employee training and enhancing the usability of the systems susceptible to misuse. Error interception focuses on better controlling workflows, introducing artificial delays, and frequent audits. In contrast, error correction focuses on timely feedback, root cause analysis, and computer-based decision support systems to assist in decision-making. By using this three-part error management program to address human error, managers can better enhance ISSP compliance within their organizations.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers &*

Security, *31*(5), 673-680. doi: 10.1016/j.cose.2012.04.004 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740481200065X

Abstract. This paper aims at surveying the extrinsic and intrinsic motivations that influence the propensity toward compliant information security behavior. Information security behavior refers to a set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies. The intention is to classify the research done on compliant information security behavior from an end-user perspective and arrange it as a taxonomy predicated on Self-Determination Theory (SDT). In addition, the relative significance of factors that contribute to compliant information security behavior is evaluated on the basis of empirical studies. The taxonomy will be valuable in providing a comprehensive overview of the factors that influence compliant information security behavior and in identifying areas that require further research.

Summary. The author of this article presents a new taxonomy, the Classification of Security Compliant Behavior, predicted on Self-determination Theory ($CSCB^{SDT}$). This work derives from the human motivation taxonomy of Ryan and Deci (2000), which draws upon their earlier work on self-determination theory (SDT) (Deci & Ryan, 1985). Ryan and Deci (1985) classify motivation as *intrinsic*, *extrinsic*, or *amotivation*, the latter being where an individual is not motivated to act due to a lack of competence or the perceived lack of value of an activity. Ryan and Deci (2000) further classify extrinsic motivation into four constructs of regulation: (1) *external*, such as the potential for reward or sanction; (2) *introjection*, where one acts to maintain self-esteem; (3) *identification*, when an individual accepts a situation as important; and (4) *integration*,

where the goal is completely incorporated with the individual's beliefs and needs. The author further develops the $CSCB^{SDT}$ by surveying the empirical literature of compliant security behavior to create a total of five ranks in the taxonomy. The third taxonomic rank of $CSCB^{SDT}$ includes *deterrent controls*, *social climate*, *awareness*, *threat appraisal*, and *coping appraisal*. The fourth taxonomic rank includes mechanisms and behavioral constructs, such as *sanctions* as a type of deterrent control. The fifth taxonomic rank includes individual attributes like *severity of punishment* for sanctions. The findings of this article provide a foundation for organizations to classify and identify the extrinsic motivations of ISSP compliance.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January 3-6). *Employees' behavior towards IS security policy compliance*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences. doi:10.1109/HICSS.2007.206 Retrieved from http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/index.html

Abstract. The literature agrees that the major threat to IS security is constituted by careless employees who do not comply with organizations' IS security policies and procedures. To address this concern, different approaches for ensuring employees' IS security policy compliance have been proposed. Prior research on IS security compliance has criticized these extant IS security awareness approaches as lacking theoretically and empirically grounded principles to ensure that employees comply with IS security policies. To fill this gap, this study proposes a theoretical model that contains the factors that explain employees' IS security policy compliance. Data (N=245) from a Finnish company provides empirical support for the model. The results suggest that information

quality has a significant effect on actual IS security policy compliance. Employees' attitude, normative beliefs and habits have significant effect on intention to comply with IS security policy. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on employees' attitude towards complying. Sanctions have insignificant effect on intention to comply with IS security policy and rewards do not have a significant effect on actual compliance with IS security policy.

Summary. To better understand the behaviors involved in ISSP compliance, the authors develop a research model using the theory of reasoned action (TRA), general deterrence theory (GDT), protection motivation theory (PMT), information systems success, and Triandis' behavioral framework (Ajzen, 1991; DeLone & MacLean, 1992; Fishbein & Ajzen, 1975; Straub, 1990; Straub & Welke, 1998; Rogers, 1983; Rippetoe & Rogers, 1987; Triandis, 1980). The TRA informs how an individual's attitude toward compliance and intention to comply influences his or her actual compliance (Fishbein & Ajzen, 1975; Ajzen, 1991). The GDT informs how the severity and timeliness of sanctions influence compliance (Straub, 1990; Straub & Welke, 1998). The PMT informs both an individual's threat appraisal of dangerous events and coping appraisal to cope with a threat and avert any negative repercussions (Rogers, 1983; Rogers & Prentice-Dunn, 1997; Rippetoe & Rogers, 1987). DeLone and MacLean (1992) define information systems success, e.g., ISSP compliance, as being influenced by information quality measured by an individual's perceived importance and usefulness of the information. Triandis' (1980) behavioral framework informs how habits and facilitating conditions, such as resources, influence intentions and attitudes towards ISSP compliance (Limayem & Hirt, 2003; McCoy &

Fowler, 2004; Triandis, 1980). In addition, the authors draw upon the constructs of rewards and normative beliefs for their model (Cameron & Pierce, 2002; Fishbein & Ajzen, 1975). From the theories, the authors derive 10 main constructs that may relate to actual ISSP compliance: *sanctions*, *threat appraisal*, *coping appraisal*, *normative beliefs*, *information quality*, *facilitating conditions*, *habits*, *rewards*, *attitude towards coping*, and *intention to comply*. To test whether these constructs contribute to actual ISSP compliance, the authors conduct a survey of 240 participants from a Finnish company. The authors use a multiple regression analysis in their study, which demonstrates the independent variables of threat appraisal ($p < 0.001$) and facilitating conditions ($p < 0.001$) both have a significant, positive effect on the dependent variable of attitude towards complying with ISSP. The independent variables of attitude towards complying ($p < 0.001$), normative beliefs ($p < 0.001$), and habits ($p < 0.05$) all have a significant, positive effect on the dependent variable of intention to comply with ISSP. Finally, the independent variables of intention to comply ($p < 0.001$) and information quality ($p < 0.05$) have a significant, positive effect on the dependent variable of actual compliance. The constructs of coping appraisal, sanctions, and rewards do not affect ISSP compliance. The findings of this study can be used to design an ISSP with focus on constructs that may increase compliance.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi: 10.1016/j.cose.2009.05.008 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740480900056X

Abstract. The ultimate success of information security depends on appropriate information security practice behaviors by the end users. Based on social cognitive theory, this study models and tests relationships among self-efficacy in information security, security practice behavior and motivation to strengthen security efforts. This study also explores antecedents to individuals' self-efficacy beliefs in information security. Results provide support for the many hypothesized relationships. This study provides an initial step toward understanding of the applicability of social cognitive theory in a new domain of information security. The results suggest that simply listing what not to do and penalties associated with a wrong doing in the users' information security policy alone will have a limited impact on effective implementation of security measures. The findings may help information security professionals design security awareness programs that more effectively increase the self-efficacy in information security.

Summary. To better understand the behaviors involved in ISSP compliance, the authors develop a research model based upon *self-efficacy* using social cognitive theory (Bandura, 1986; Ozer & Bandura, 1990). Self-efficacy addresses an individual's belief in his/her own ability to accomplish a task or reach a goal (Bandura, 1986; Ozer & Bandura, 1990). Bandura (1997) advises that researchers consider the context of self-efficacy when attempting to measure its effect. Rhee, Kim, and Ryu (2009) address this by defining self-efficacy in information security (SEIS) as "a belief in one’s capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (p. 818). From social cognitive theory, the authors hypothesize that the following factors influence SEIS: (1) previous *computer/Internet*

experience, (2) previous experiences with *security breach incidents*, and (3) the perception of having *general controllability* over information security threats. The authors also present a second set of hypotheses where individuals with higher SEIS (1) engage in the use of more *security practice – technology* such as protection software; (2) demonstrate more *security practice – care behavior* in the form of ISSP compliance; and (3) demonstrate a *long-term intention to strengthen security effort* through activities, such as continuing information security education. To test these hypotheses, the authors conduct a survey with 415 graduate students majoring in business. The authors use a partial least squares regression analysis in their study with the dependent variable of SEIS for the first set of hypotheses. Computer/Internet experience ($p < 0.001$) and general controllability ($p < 0.01$) as independent variables are shown to have a significant, positive influence on SEIS. However, the independent variable of previous experience with security breach incidents ($p < 0.05$) has a significant negative effect on SEIS. The second set of hypotheses that the independent variable of SEIS positively influences the dependent variables of security practice – technology ($p < 0.001$), security practice – care behavior ($p < 0.001$), and intention to strengthen security efforts ($p < 0.001$) are supported. The results of this study can be used in development of SEIS training to enhance ISSP compliance.

Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. doi: 10.1016/j.im.2011.07.002 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720611000681

Abstract. Given the significant role of people in the management of security, attention has recently been paid to the issue of how to motivate employees to improve security performance of organizations. However, past work has been dependent on deterrence theory rooted in an extrinsic motivation model to help understand why employees do or do not follow security rules in their organization. We postulated that we could better explain employees' security-related rule-following behavior with an approach rooted in an intrinsic motivation model. We therefore developed a model of employees' motivation to comply with IS security policies which incorporated both extrinsic and intrinsic models of human behavior. It was tested with data collected through a survey of 602 employees in the United States. We found that variables rooted in the intrinsic motivation model contributed significantly more to the explained variance of employees' compliance than did those rooted in the extrinsic motivation model.

Summary. The author of this study develops a research model using both intrinsic and extrinsic motivations to better understand how they influence ISSP compliance. Intrinsic motivation hypotheses test the influence of an individual's *perceived legitimacy* of ISSP and *perceived value congruence*, i.e., employers and employees sharing the same value set, on ISSP compliance (Tyler, 2006; Tyler & Blader, 2005). Using general deterrence theory, extrinsic motivation hypotheses test the influence of an individual's *perceived deterrent certainty* and *perceived deterrent severity* of sanctions on ISSP non-compliance (Straub, 1990; Straub & Welke, 1998). The influences of control variables, such as gender and computer self-efficacy, on ISSP compliance are also examined. To test these hypotheses, the author conducts a survey with a nation-wide sample of 602 participants. The authors use a partial least squares regression analysis in their study with the

dependent variable of ISSP *compliance*. The intrinsic motivations of perceived legitimacy ($p < 0.001$) and value congruence ($p < 0.05$) as independent variables both positively influence ISSP compliance. In contrast, the extrinsic motivations of perceived deterrent certainty and severity as independent variables have no significant influence on ISSP compliance. Further, the independent control variable of computer self-efficacy ($p < 0.05$) has a significant, positive influence on ISSP compliance. The implications from this study are that organizations should focus on aligning organizational ISSP values with employee values to increase compliance. Moreover, information security training and education increases the perceived legitimacy of ISSP.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198. doi: 10.1016/j.im.2012.04.002 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720612000328

Abstract. Employees' failure to comply with IS security procedures is a key concern for organizations today. A number of socio-cognitive theories have been used to explain this. However, prior studies have not examined the influence of past and automatic behavior on employee decisions to comply. This is an important omission because past behavior has been assumed to strongly affect decision-making. To address this gap, we integrated habit (a routinized form of past behavior) with Protection Motivation Theory (PMT), to explain compliance. An empirical test showed that habitual IS security compliance strongly reinforced the cognitive processes theorized by PMT, as well as employee intention for future compliance. We also found that nearly all components of PMT

significantly impacted employee intention to comply with IS security policies. Together, these results highlighted the importance of addressing employees' past and automatic behavior in order to improve compliance.

Summary. The authors develop a research model using protection motivation theory (PMT) and habit, i.e., routinized behavior, to explain ISSP compliance (Limayem & Hirt, 2003; Rogers, 1983; Verplanken & Orbell, 2003). The PMT informs both an individual's threat appraisal of dangerous events and coping appraisal to cope with a threat and avert any negative repercussions (Rogers, 1983). The instrument of Verplanken and Orbell (2003) examines the concept of habit; this instrument addresses not only behavioral frequency but also *automaticity*, i.e., performing an action without a conscious decision. From the PMT, the authors develop a set of hypotheses that the following constructs influence an individual's intention to comply with ISSP: (1) assessment of organizational *vulnerability* to threats, (2) *perceived severity* of threats, (3) the *rewards* of saving time by not complying with ISSP, (4) *response efficacy* as the belief a protective behavior will avoid a threat, (5) individual *self-efficacy* in implementing a protective behavior, and (6) *response cost* of implementing a protective behavior. An additional set of hypotheses examines the influence of habit on the six PMT hypotheses. To test these hypotheses, the authors conduct a survey of 210 participants, representing clerical and administrative staff from a Finnish, municipal organization and perform a partial least squares regression analysis of the data from the survey results. The independent variable of habit has a significant influence on all six dependent variable constructs of PMT ($p < 0.03$) as they relate to the intention to comply with ISSP. The independent variables of perceived severity ($p < 0.01$) and self-efficacy ($p < 0.01$) have a positive effect on the dependent

variable of intention to comply with ISSP, whereas the independent variables of rewards ($p < 0.03$), response efficacy ($p < 0.01$), and response cost ($p < 0.05$) have a negative effect on the intention to comply. The independent variable of assessed vulnerability has no effect on the intention to comply. Thus, the intention to comply with ISSP increases by improving the usability systems that enact ISSP. In addition, compliance may increase with IS security education that stresses the potential vulnerability and severity of threats.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198. doi: 10.1016/j.cose.2004.01.012 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740480400032X

Abstract. Auditing has always played an important role in the business environment. With the introduction of information technology and the resulting security challenges that organizations face daily, it has become essential to ensure the security of the organization's information and other valuable assets. However, one aspect that auditing does not cover effectively is that of the behaviour of the employee, which is so crucial to any organization's security. The objective of this paper is to explore the potential problems concerning the attempt to audit the behaviour of the employee. It will be demonstrated that it is extremely difficult to audit human behaviour and so an alternative method to behavioural auditing needs to be found, where policing the employee is not necessary, but instead a softer, more informal approach is used to change the culture to a more information security conscious one.

Summary. This article addresses the challenges of auditing employee behavior and offers an alternative method to improve organizational ISSP compliance. The authors

examine the evaluation of employee behavior in the context of performance appraisals. Performance appraisals may lack *reliability* and *validity*, leading to unreliable information (Szilagyi & Wallace, 1990), and numerous factors distort actual from assessed performance (Cooper, 1981). The authors propose a means to address organizational culture so that employee behavior is in line with organizational objectives like ISSP compliance. They recognize Schein's (1999) model of organizational culture, which defines three layers: (1) *artifacts and creations*; (2) *espoused values, norms, and knowledge*; and (3) *basic assumptions and beliefs* or *tacit assumptions*. The authors suggest that changing these layers to be more in line with ISSP compliance can result in employees adjusting their behaviors towards greater ISSP compliance. Additionally, Szilagyi and Wallace (1990) categorize organizational behavior into three levels: *individual, group,* and *formal organization*. Each level influences the other, and all three must improve their influence on ISSP compliance in order to guide the culture of the organization towards greater ISSP compliance (Szilagyi & Wallace, 1990). Schein's (1999) Organizational Culture Model demonstrates its interaction with Szilagyi and Wallace's (1990) categories and informs focus areas to increase ISSP compliance. The findings of this study provide a model for managers to improve individual employee ISSP compliance without direct auditing by addressing the organizational culture as a whole.

Conclusion

This annotated bibliography summarizes literature addressing employee behavioral factors that influence ISSP compliance. Relevant literature regarding behavioral constructs in the areas of biases, beliefs, perceptions, and motivations are summarized. The research goal of this annotated bibliography is to examine the employee behavioral factors on which managers should focus within their organizations to improve ISSP compliance.

Employee behavior is often considered the "weakest link" in information security (Huang, Rau, & Salvendy, 2007; Ifinedo, 2014; Warkentin & Willison, 2009). Addressing employee behaviors is important, as information security cannot be achieved exclusively by technological means (Herath & Rao, 2009). ISSP allows for the influence of employee behaviors as they pertain to the use of organizational information systems (Ifinedo, 2012). Managers play a key role in supporting organizational ISSP compliance due to their influence (Ifinedo, 2014; Pahnila, Siponen, & Mahmood, 2007; Ruighaver, Maynard, & Chang, 2007). Managers can improve ISSP compliance by focusing on the following behavioral constructs and social contexts.

Human Error

Numerous perception biases may influence an individual's incorrect assessment of and response to security risks. A report from the Australian Government, Department of Defence, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organization (2010) highlights several theories related to perception biases as they apply to failed ISSP compliance, which are listed in the table below.

Table 1

Perception biases of security risks and their impact on ISSP compliance.

Theory	**Description**	**References**
Availability heuristic	Misunderstanding the likelihood and importance of a current event based upon its memorability, leading to inappropriate responses, e.g., underestimating the day-to-day impact of poor ISSP procedures as opposed to a one-time, dramatic hacking incidence.	Slovic, Fischhoff, & Lichtenstein, 1979; Tversky & Kahneman, 1973
Optimism bias	The belief that negative events will happen to others and not to themselves, e.g., individuals think that they would not be the target of hackers because they don't manage sensitive information resulting in lower ISSP compliance.	McIlwraith, 2006; Sjöberg, 2000; Weinstein, 1987
Level of control	Individuals may underestimate the significance of a security risk if they believe that they can control their environments. An overestimation of control can result in individuals taking more security risks.	Kreuter & Strecher, 1995; Slovic, Fischhoff, & Lichtenstein, 1978
Level of knowledge	Lack of knowledge about a security risk can bias an individual's assessment, which in turn leads to an inappropriate or ineffective response.	Fischhoff, 2002; Lacohée, Phippen, & Furnell, 2006
Risk homeostasis	As a situation changes, individuals adjust their behaviors accordingly to maintain a specific level of exposure to risk. Incomplete understanding of new security situations may lead to increased risk-taking behaviors.	Stewart, 2004; Wilde, 2001
Cumulative risk	Individuals may not be aware that taking small security risks can accumulate into a larger, additive risk over time.	Fischhoff, 2002; Slovic, 2000
Omission bias	Failing to comply with ISSP is perceived to be less of an issue than a direct violation of ISSP, e.g., failing to periodically change a password is less of an infraction than writing it down.	Ritov & Baron, 1992
Influence of framing	Risk-taking behaviors may increase if only the negative effects of ISSP non-compliance are communicated as opposed to potential security gains.	Kahneman & Tversky, 1979

Human factors, such as perception biases, are not completely avoidable; therefore, the best course of action is to acknowledge their potential effects and develop mitigation strategies to improve ISSP compliance. Liginlal, Sim, and Khansa (2009) suggest using a three-part defense-

in-depth error management strategy to address causes of human error: (1) *error avoidance* focusing on employee training and enhancing the usability of the systems susceptible to misuse; (2) *error interception* focusing on frequent audits, better control of workflows with additional security checks and cross-verification by peers or supervisors, and introducing artificial delays to allow employees to self-detect errors they have committed; and (3) *error correction* focusing on timely feedback, root-cause analysis, and computer-based decision support systems to assist in decision making.

Beliefs and Perceptions

The following areas demonstrate a positive influence on ISSP compliance:

Attitude. Employee beliefs about the outcomes of ISSP compliance and noncompliance have a direct impact on their attitudes, which influence ISSP compliance (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009). Subjective and personal norms, along with the perceived vulnerability and severity of security threats, are also shown to have an effect on employee attitudes, thereby influencing ISSP compliance (Ifinedo, 2014; Pahnila, Siponen, & Mahmood, 2007). Creating a culture of information security awareness (ISA) through repeated training sessions, regular meetings, and IS campaigns can help improve employee attitudes (Bulgurcu, Cavusoglu, & Benbasat, 2010; Ifinedo, 2012; Pahnila, Siponen, & Mahmood, 2007; Son, 2011). Training should focus on the benefits of compliance, the costs of compliance, and the costs of noncompliance (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Normative beliefs. Social influence, expectations, and pressure from peers and superiors directly influence ISSP compliance (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Pahnila, Siponen, & Mahmood, 2007). To promote ISSP compliance, managers should foster a security climate by making their expectations clear, highlighting the importance of ISSP

compliance, and reiterating that employee efforts make a difference in achieving organizational security goals (Herath & Rao, 2009; Pahnila, Siponen, & Mahmood, 2007). Managers can also influence normative beliefs by identifying influential people within the organization and empowering them with the role of ISSP champion (Ifinedo, 2012, 2014). Ifinedo (2014) also notes that individuals are more likely to comply with ISSP when the topic is addressed as a social issue that impacts their coworkers. Hosting ISA sessions and providing regular ISSP training influence individual beliefs that in turn positively influence normative beliefs (Ifinedo, 2014).

Self-efficacy. *Self-efficacy theory* addresses an individual's belief in his/her ability to and knowledge of how to follow and achieve ISSP compliance (Bandura, 1977; Bulgurcu, Cavusoglu, & Benbasat, 2010; Rhee, Kim, & Ryu, 2009). Importantly, training provides the knowledge, skills, and hands-on practice to ensure that employees can confidently achieve ISSP compliance and believe in their abilities to do so (Bulgurcu, Cavusoglu, & Benbasat, 2010). To improve self-efficacy, managers should support employees with time and resources to learn new security-related technologies and skills that directly benefit the organization's ISSP goals (Ifiendo, 2012).

Positive Extrinsic Motivations

The following factors are shown to provide positive extrinsic motivations and have a positive influence on ISSP compliance:

Reducing the perceived costs of compliance. Employees who perceive ISSP compliance as interfering with their daily job or as a burden may be less motivated to comply (Bulgurcu, Cavusoglu, & Benbasat, 2010). Managers can increase compliance by clearly allocating a portion of employee time to achieve compliance and reducing the perception that

compliance activities interfere with job duties (Bulgurcu, Cavusoglu, & Benbasat, 2010). Managers can also increase ISSP compliance by promoting usability reviews to ensure that organizational ISSP is streamlined, efficient, relevant, and not perceived as cumbersome (Bulgurcu, Cavusoglu, & Benbasat, 2010; Vance, Siponen, & Pahnila, 2012).

Improved threat appraisal. The constructs of *perceived vulnerability* to and *perceived severity* of information security threats comprise the concept of threat appraisal (Pahnila, Siponen, & Mahmood, 2007). Research shows that an increase of these two perceptions independently or together can have a positive influence on ISSP compliance (Huang, Rau, & Salvendy, 2007; Ifinedo, 2012; Pahnila, Siponen, & Mahmood, 2007; Vance, Siponen, & Pahnila, 2012). To increase ISSP compliance, managers need to make employees aware of potential vulnerabilities and resulting severe consequences, which can be accomplished through seminars, training sessions, posters, and email (Ifinedo, 2012; Pahnila, Siponen, & Mahmood, 2007; Vance, Siponen, & Pahnila, 2012).

Personal responsibility and informal workgroup sanctions. Employees who feel personal responsibility to comply with ISSP are shown to have reduced intentions to violate ISSP (Guo & Yuan, 2012). Managers can increase feelings of responsibility by focusing on ISSP training as it directly relates to business risks as opposed to ISSP training with little or no business context (Guo & Yuan, 2012). Workgroups influence individual employees by expressing disapproval of an individual's intentions to violate ISSP (Guo & Yuan, 2012). Managers can increase the positive influence of workgroups by training security role models who advocate behaviors related to ISSP compliance (Guo & Yuan, 2012).

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211. doi: 10.1016/0749-5978(91)90020-T Retrieved from http://www.sciencedirect.com/science/article/pii/074959789190020T

Australian Government, Department of Defence, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organization. (2010). *Human factors and information security: Individual, culture and security environment*. (DSTO-TR-2484). Retrieved from http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10094/1/DSTO-TR-2484%20PR.pdf

Acquisti, A., Friedman, A., & Telang, R. (2006, June 26-28). *Is there a cost to privacy breaches? An event study*. Paper presented at the Fifth Workshop on the Economics of Information Security (WEIS 2006), Robinson College, University of Cambridge, England. Retrieved from http://weis2006.econinfosec.org/prog.html

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215. Retrieved from http://psycnet.apa.org/psycinfo/2000-07436-014

Bandura A. (1986). *Social foundations of thoughts and action: a social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura A. (1997). *Self-efficacy-the exercise of control*. New York: W.H. Freeman and Company.

Bell, C., & Frantz, P. (2013, July). Critical evaluation of information sources. Retrieved from http://library.uoregon.edu/guides/findarticles/credibility.html

Berzkalne, I., & Zelgalve, E. (2014). Intellectual capital and company value. *Procedia-Social and Behavioral Sciences, 110*, 887-896. doi: 10.1016/j.sbspro.2013.12.934 Retrieved from http://www.sciencedirect.com/science/article/pii/S1877042813055742

Bontis, N. (2001). Assessing knowledge assets: a review of the models used to measure intellectual capital. *International journal of management reviews, 3*(1), 41-60. doi: 10.1111/1468-2370.00053 Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/1468-2370.00053/abstract

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3). Retrieved from http://www.academia.edu/download/30986994/bulgurcucavusoglubenbasat.pdf

Cameron, J., & Pierce, W. (2002). *Rewards and intrinsic motivation: Resolving the controversy*. Westport, CT: Bergin & Garvey.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448. Retrieved from http://iospress.metapress.com/content/5nkxhffc775tuel9/

Cooper, W. H. (1981). Ubiquitous halo. *Psychological bulletin, 90*(2), 218. doi: 10.1037/0033-2909.90.2.218 Retrieved from http://psycnet.apa.org/journals/bul/90/2/218/

Covello, V. T. (1983). The perception of technological risks: A literature review. *Technological Forecasting and Social Change, 23*(4), 285-297. doi: 10.1016/0040-1625(83)90032-X Retrieved from http://www.sciencedirect.com/science/article/pii/004016258390032X

Covello, V. T. (1992). Risk communication: An emerging area of health communication

research. *Communication yearbook, 15*(1), 359-373.

Covello, V. T., & Merkhofer, M. W. (1993). *Risk assessment methods: Approaches for assessing health and environmental risks*. New York: Plenum Press.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York: Plenum.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information systems research, 3*(1), 60-95. doi: 10.1287/isre.3.1.60 Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/isre.3.1.60

Digital Object Identifier System. (2014, March 17). DOI handbook. Retrieved from http://www.doi.org/hb

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review, 14*(1), 57-74. doi: 10.5465/AMR.1989.4279003 Retrieved from http://amr.aom.org/content/14/1/57.short

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fischhoff, B. (2002). Assessing and communicating the risks of terrorism. In A. H. Teich S. D. Nelson S. J. Lita (Eds.), S*cience and technology in a vulnerable world* (pp. 51-64). Washington, DC: American Association for the Advancement of Science. Retrieved from http://www.aaas.org/sites/default/files/migrate/uploads/stvw.pdf

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe

enough? A psychometric study of attitudes towards technological risks and benefits. *Policy sciences, 9*(2), 127-152. doi: 10.1007/BF00143739 Retrieved from http://link.springer.com/article/10.1007/BF00143739

Glazer, R. (1991). Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. *The Journal of Marketing*, 1-19. doi: 10.2307/1251953 Retrieved from http://www.jstor.org/stable/1251953

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404-410. doi: 10.1016/j.im.2009.06.005 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720609000895

Guo, K. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security,* 32, 242-251. doi: 10.1016/j.cose.2012.10.003 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404812001666

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. doi: 10.1016/j.im.2012.08.001 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720612000584

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167923609000530

Hirschi, T. (2002). *Causes of delinquency*. New Brunswick, NJ: Transaction publishers.

Höne, K., & Eloff, J. H. P. (2002). Information security policy – what do international information security standards say? *Computers & Security, 21*(5), 402-409. doi: 10.1016/S0167-4048(02)00504-7 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404802005047

Huang, D., Rau, P.P. & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. Jacko (Ed.). Human-Computer Interaction, Part IV (pp. 906-915). Heidelberg: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-73111-5_100

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404811001337

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720613000980

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 263-291. Retrieved from http://www.jstor.org/stable/1914185

Kakabadse, N. K., Kouzmin, A., & Kakabadse, A. (2001). From tacit knowledge to knowledge management: Leveraging invisible assets. *Knowledge and Process Management, 8*(3), 137-154. doi: 10.1002/kpm.120 Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/kpm.120/full

Kreuter, M. W., & Strecher, V. J. (1995). Changing inaccurate perceptions of health risk: Results from a randomized trial. *Health Psychology*, *14*(1), 56. doi: 10.1037/0278-6133.14.1.56 Retrieved from http://psycnet.apa.org/journals/hea/14/1/56/

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296. doi:10.1016/j.cose.2006.02.008 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404806000563

Lacohée, Hazel, Andrew D. Phippen, & Steven M. Furnell. Risk and restitution: Assessing how users establish online trust. *Computers & Security* 25.7 (2006): 486-493. doi: 10.1016/j.cose.2006.09.001 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404806001489

Lawton, G. (2007). Web 2.0 creates security challenges. *Computer*, *40*(10), 13-16. doi: 10.1109/MC.2007.367 Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4343682

Lee, W., Fan, W., Miller, M., Stolfo, S. J., & Zadok, E. (2002). Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, *10*(1), 5-22. Retrieved from http://academiccommons.columbia.edu/item/ac:125810

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., & Combs, B. (1978). Judged frequency of lethal events. *Journal of experimental psychology: Human learning and memory*, *4*(6), 551-578. doi: 10.1037/0278-7393.4.6.551 Retrieved from http://psycnet.apa.org/journals/xlm/4/6/551.pdf

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy

breaches? An empirical study and a framework for error management. *Computers & Security, 28*(3), 215-228. doi: 10.1016/j.cose.2008.11.003 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808001181

Lumayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems, 4*(1), 65-95. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=16701826&site=ehost-live&scope=site

McCoy, C., & Fowler, R. T. (2004, October). You are the key to security: Establishing a successful security awareness program. In *Proceedings of the 32nd annual ACM SIGUCCS fall conference* (pp. 346-349). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1027882

McIlwraith, A. (2006). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Gower Publishing, Ltd..

O'Reilly, T. (2007). What is Web 2.0? Design patterns and business models for the next generation of software. *Communications & Strategies, 1*, 17-17. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1008839

Ozer, E. M., & Bandura, A. (1990). Mechanisms governing empowerment effects: A self-efficacy analysis. *Journal of personality and social psychology, 58*(3), 472. doi: 10.1037/0022-3514.58.3.472 Retrieved from http://psycnet.apa.org/journals/psp/58/3/472/

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers &*

Security, *31*(5), 673-680. doi: 10.1016/j.cose.2012.04.004 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740481200065X

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January 3-6). *Employees' behavior towards IS security policy compliance*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences. doi:10.1109/HICSS.2007.206 Retrieved from http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/index.html

Ponemon Institute, LLC. (2013, May 28). 2013 Cost of data breech: Global analysis. Retrieved from http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

Reason J. (1990). *Human error*. New York, NY: Cambridge University Press.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. doi: 10.1016/j.cose.2009.05.008 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740480900056X

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of personality and social psychology*, *52*(3), 596. doi: 10.1037/0022-3514.52.3.596 Retrieved from http://psycnet.apa.org/journals/psp/52/3/596/

Ritov, I., & Baron, J. (1992). Status-quo and omission biases. *Journal of Risk and Uncertainty*, *5*(1), 49-61. doi: 10.1007/BF00208786 Retrieved from http://link.springer.com/article/10.1007/BF00208786

Rogers R. (1983). Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social psychophysiology: a sourcebook* (pp. 153-176). New York: Guilford Press.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research I: Personal and social determinants* (pp. 113-132). New York, NY: Plenum Press.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological monographs: General and applied, 80*(1), 1. doi: 10.1037/h0092976 Retrieved from http://psycnet.apa.org/journals/mon/80/1/1/

Roy Rosenzweig Center for History and New Media. (2014a). About. Retrieved from https://www.zotero.org/about/

Roy Rosenzweig Center for History and New Media. (2014b). Adding items to your Zotero library. Retrieved from https://www.zotero.org/support/getting_stuff_into_your_library

Roy Rosenzweig Center for History and New Media. (2014c). Adding files to your Zotero library. Retrieved from https://www.zotero.org/support/attaching_files

Roy Rosenzweig Center for History and New Media. (2014d). Collections and tags. Retrieved from https://www.zotero.org/support/collections_and_tags

Roy Rosenzweig Center for History and New Media. (2014e). Notes. Retrieved from https://www.zotero.org/support/notes

Roy Rosenzweig Center for History and New Media. (2014f). Zotero Standalone (Version 4.0.19) [Computer software]. Fairfax, VA: George Mason University. Retrieved from https://www.zotero.org/download/

Ruighaver, A., Maynard, S. , & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62. doi:10.1016/j.cose.2006.10.008 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740480600157X

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology*, *25*(1), 54-67. doi: 10.1006/ceps.1999.1020 Retrieved from http://www.sciencedirect.com/science/article/pii/S0361476X99910202

Schein E. (1999). *The corporate culture survival guide*. San Francisco, CA: Jossey-Bass Publishers.

Sjöberg, L. (2000). Factors in risk perception. *Risk analysis*, *20*(1), 1-12. doi: 10.1111/0272-4332.00001 Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.00001/abstract

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285. doi: 10.1126/science.3563507 Retrieved from http://www.sciencemag.org/content/236/4799/280.short

Slovic, P. (2000). What does it mean to know a cumulative risk? Adolescents' perceptions of short- term and long- term consequences of smoking. *Journal of Behavioral Decision Making*, *13*(2), 259-266. doi: 10.1002/(SICI)1099-0771(200004/06)13:2<259::AID-BDM336>3.0.CO;2-6 Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/(SICI)1099-0771(200004/06)13:2%3C259::AID-BDM336%3E3.0.CO;2-6/abstract

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1978). Accident probabilities and seat belt usage: A psychological perspective. *Accident Analysis & Prevention*, *10*(4), 281-285. doi: 10.1016/0001-4575(78)90030-1 Retrieved from http://www.sciencedirect.com/science/article/pii/0001457578900301

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the risks. *Environment*, *21*, 14-20, 36-39.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears - Understanding risk. In R.C. Schwing & W.A. Albers (Eds.), *Societal risk assessment - How safe is safe enough?* (pp. 181-218). New York: Plenum.

Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. doi:10.1016/j.im.2011.07.002 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720611000681

Stewart, A. (2004). On risk: Perception and direction. *Computers & Security, 23*(5), 362-370. doi: 10.1016/j.cose.2004.05.003 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404804001233

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 2*(44), 441-469. Retrieved from http://www.jstor.org/stable/249551

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276. doi: 10.1287/isre.1.3.255 Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/isre.1.3.255

Szilagyi A. D., & Wallace, M.J. (1990). *Organizational behavior and performance* (5th ed.). Glenview, IL: Scott Foresman and Company.

Thomson, K. , & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69-75. doi:10.1016/j.cose.2004.10.005 Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404804002627

Triandis, H. C. (1979). *Values, attitudes, and interpersonal behavior*. In Nebraska symposium on motivation (pp. 195-259). Lincoln, NE: University of Nebraska Press.

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology, 57*, 375-400. doi: 10.1146/annurev.psych.57.102904.190038 Retrieved from http://www.annualreviews.org/doi/abs/10.1146/annurev.psych.57.102904.190038

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143-1158. doi: 10.5465/AMJ.2005.19573114 Retrieved from http://amj.aom.org/content/48/6/1143.short

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology, 5*(2), 207-232. doi: 10.1016/0010-0285(73)90033-9 Retrieved from http://www.sciencedirect.com/science/article/pii/0010028573900339

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198. doi: 10.1016/j.im.2012.04.002 Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720612000328

Vanhecke, T. E. (2008). Zotero. *Journal of the Medical Library Association : JMLA*, 96(3), 275–276. doi:10.3163/1536-5050.96.3.022 Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2479046/

Verplanken, B., & Orbell, S. (2003). Reflections on past Behavior: A self- report index of habit strength. *Journal of Applied Social Psychology, 33*(6), 1313-1330. doi: 10.1111/j.1559-1816.2003.tb01951.x Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2003.tb01951.x/abstract

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance.

Computers & Security, *23*(3), 191-198. doi: 10.1016/j.cose.2004.01.012 Retrieved from http://www.sciencedirect.com/science/article/pii/S016740480400032X

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18(*2), 101-105. Retrieved from http://www.researchgate.net/publication/220393124_Behavioral_and_policy_issues_in_information_systems_security_the_insider_threat/file/32bfe50f990ef27317.pdf

Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of behavioral medicine*, *10*(5), 481-500. doi: 10.1007/BF00846146 Retrieved from http://link.springer.com/article/10.1007/BF00846146

Wiig, K. M. (1997). Integrating intellectual capital and knowledge management. *Long range planning*, *30*(3), 399-405. doi: 10.1016/S0024-6301(97)90256-9 Retrieved from http://www.sciencedirect.com/science/article/pii/S0024630197902569

Wilde, G.J.S. (2001). *Target Risk 2: A new psychology of safety and health.* Toronto: PDE Publications.

Wilson, R. M., & Stenson, J. A. (2008). Valuation of information assets on the balance sheet: The recognition and approaches to the valuation of intangible assets. *Business Information Review*, *25*(3), 167-182. doi: 10.1177/0266382108095039 Retrieved from http://bir.sagepub.com/content/25/3/167.short

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of

information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. doi: 10.1016/j.chb.2008.04.005 Retrieved from http://www.sciencedirect.com/science/article/pii/S0747563208000824