Studies on Employees' Information Security Awareness

Dissertation

zur Erlangung des wirtschaftswissenschaftlichen Doktorgrades
der Wirtschaftswissenschaftlichen Fakultät der Georg-August-Universität Göttingen

vorgelegt von
Felix Häußinger
geboren in München

Göttingen, 2015

Erstgutachter:	Prof. Dr. Johann Kranz
Zweitgutachter:	Prof. Dr. Lutz M. Kolbe
Drittgutachter:	Prof. Dr. Jan Muntermann
Tag der mündlichen Prüfung:	13. Mai 2015

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

AMCIS = American Conference on Information Systems

ATT = Attitude

AVE = Average Variance Extracted

CA = Cronbach Alpha

CAGR = Compounded Annual Growth Rate

CIA = Confidentiality, Integrity, and Availability

COBIT = Control Objectives for Information and Technology

CR = Composite Reliability / Construct Reliability

CSIS = Centre for Strategic and International Studies

DPMA = Data Processing Management Association

ECIS = European Conference on Information Systems

ENISA = European Network and Information Security Agency

GDP = General Domestic Product

GDT = General Deterrence Theory

GISA = General Information Security Awareness

GMITS = Guidelines for the Management of IT Security

ICIS = International Conference on Information Systems

ICT = Information- and Communication Technology

InfoSec = Information Security

INT = Intention to comply

IS = Information Systems

ISA = Information Security Awareness

ISF = Information Security Forum

ISM = Information Security Management

ISMS = Information Security Management System

ISP = Information Security Policy

ISPA = Information Security Policy Awareness

ISPP = Information Security Policy Provision

ISS = Information Systems Security

IT = Information Technology

ITIL = Information Technology Infrastructure Library

IV = Independent Variable

MISA = Managerial Information Security Awareness

NIST = National Institute of Standards and Technology

OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation

OIT = Organismic Integration Theory

PLS = Partial Least Square

PMT = Protection Motivation Theory

RQ = Research Question

SCT = Social Cognitive Theory

SDT = Self-Determination Theory

SETA = Security Education Training Awareness

SSE-CMM = System Security Engineering Capability Maturity Model

TAM = Technology Acceptance Model

TPB = Theory of Planned Behavior

A. General Introduction

"What I found personally to be true was that it's easier to manipulate people rather than technology."

-- Kevin Mitnick

The emergence of the TCP/IP Internet protocol, in 1973, and the myriad connections forged by technologies such as computing devices, smartphones, networks, wireless links and other information technology (IT) infrastructure have brought tremendous benefits and opportunities to people and businesses worldwide. The fast progress of global networking and the societal penetration of information- and communication technologies (ICT) as well as the increasing reliance on information systems (IS) have made the management of critical infrastructures (e.g., healthcare, energy, finance, logistics, administration, etc.) more efficient than ever before.

But there is a darker side of this evolution, too. As a result of the connected world and the strong reliance on IS, private and public institutions have become increasingly vulnerable to cyber attacks, data theft and loss of critical business information, an asset, which is considered to be the backbone of an organization (Qudaih et al. 2014). As numerous prominent incidents in the recent past show, deficits of organizations' information systems security (ISS) can have severe consequences for society and economy. Cyber-attacks from outside the company, as well as insider threats and unintentional misbehavior committed by employees can cause a broad diversity of damage, such as financial loss, loss of customers and business partners, decrease of the firm's market value, loss of reputation or even governmental sanctions (Goel and Shawky 2009, PWC 2013). According to a recent estimate by the Centre for Strategic and International Studies (CSIS), a think-tank, cyber crime and intellectual-property theft causes an annual global loss of $445 billion – a sum that roughly equals the GDP of a smallish, wealthy European country, such as Austria (The Economist 2014). As a result, organizations around the world reportedly spent more than $ 67 billion on information security in 2014, according to the research firm Gartner (The Economist 2014). Small- and medium-size organizations are even expected to spend more on information security than on other IS/IT over the next three years (Perlroth and Rusli 2012).

Previous attempts to ensure information security have largely focused on technological remedies, such as encryption, anti-spyware, virus detection, or firewalls (Stanton et al. 2005, Spears and Barki 2010). Investing in technological ISS countermeasures, however, is not enough, since it is assumed that 50 - 70 % of overall information security incidents in organizations result either directly or indirectly from employees' misuse - ranging from naïve mistakes to intentional harm (Ernst and Young 2003, Siponen and Vance 2010). Improving information security therefore needs investments in both technical and socio-organizational resources (Bulgurcu et al. 2010). Against this background, scholars and practitioners recently shifted their attention to the human dimension of information security by applying principles of behaviorism and social psychology.

In this regard, employees' information security awareness (ISA) has been identified to be one of the most essential prerequisites of information security behavior and to play a key role in employees' policy compliance (Siponen 2000, Dinev and Hu 2007, Bulgurcu et al. 2010, Al-Omari et al. 2012). ISA is most frequently referred to as a cognitive state of mind, which is characterized by recognizing the importance of information security and being aware and conscious about ISS objectives, risks and threats, and having an interest in acquiring the required knowledge to use IS responsibly (Straub and Welke 1998, Thomson and von Solms 1998, Siponen 2000). If individuals have high levels of ISA, not only do they better know and understand information security risks, but they also make more effort overall to help keep company information secure (Siponen 2000). On the one hand, this means that employees defend the company's information against attacks and illegal information retrieval from outside the company. Whilst on the other hand, it means that employees are less likely to abuse the easy access they have to corporate confidential information, thereby preventing them from becoming the threat that the company is trying to protect itself against (Straub 1990). ISA is respected as a highly significant indicator for the overall performance of organizational information security management (ISM) practices (Hu and Dinev 2005, Choi et al. 2008) and a main element of successful ISS strategies (Cavusoglu et al. 2009, Bulgurcu et al 2010). Also, the international standard and code of best practice for ISM ISO/IEC 27001 (2005, 2013) suggests that management duties include ensuring that employees, contractors and third party users achieve a level of awareness on information security relevant to their roles and responsibilities within the organization. Although the importance of

employee's ISA has largely been recognized, recent studies indicate that ISA still remains a problematic topic, and that most employees lack an awareness of security issues, policies, and procedures (Pahnila et al. 2007a, Lim et al. 2010).

Research Questions, Contributions and Structure of the Dissertation

The purpose of this cumulative dissertation is to expand our body of knowledge according to different aspects of employees' ISA. Therefore it encompasses three interrelated studies, each of which formulates a series of research questions directed at different aspects of the topic, and gives a separate detailed discussion of the findings and their implications for research and practice. The first study is an extensive review of the existing body of ISA literature, whereas study 2 and 3 are quantitative empirical examinations of proposed research models addressing different gaps in ISA research.

The first paper develops a synthesized up-to-date review of the current state of ISA literature, with the aim to provide quick, structured access to the accumulated knowledge of ISA research, to give implications for scholars and practitioners and to reveal potential areas for further research (Webster and Watson 2002). 131 selected ISA publications are identified and analyzed. By using open coding techniques based on grounded theory – which aims to break down a topic into logical subcategories – a classification scheme is developed that categorizes five main objectives of ISA research. An overview table is given showing which publication covers which criterion (1-5), whereas one publication can cover multiple criteria. Figure 1 illustrates the classification scheme of the ISA literature.

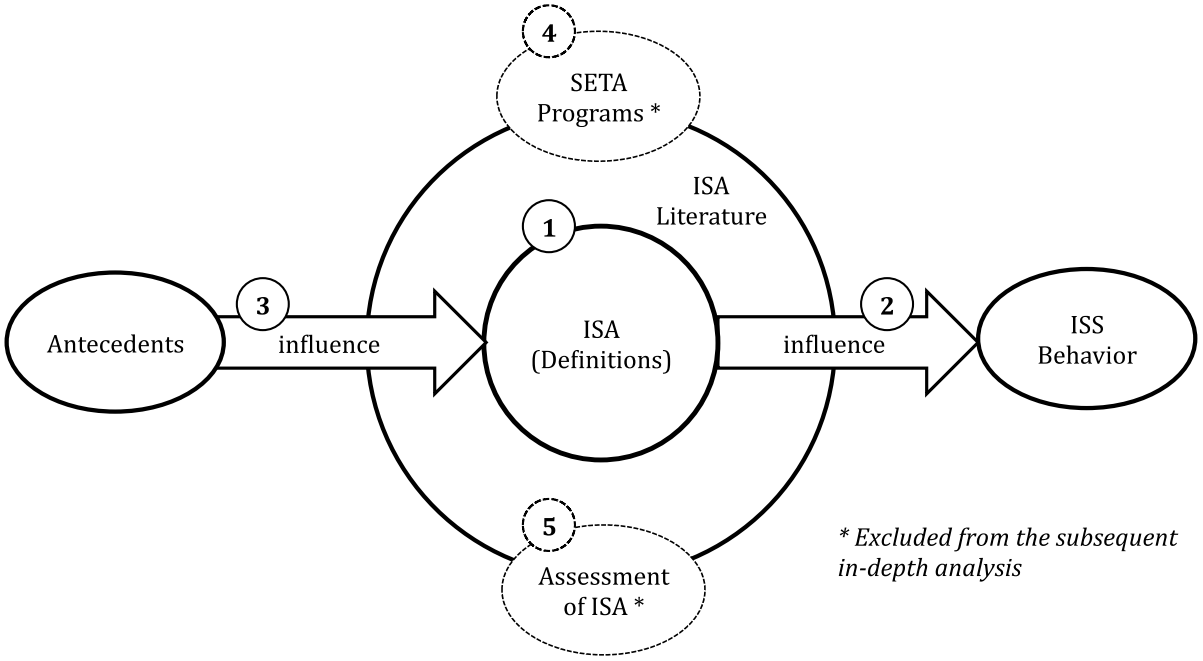


Figure 1: Classification Scheme of ISA Literature

Criterion 1 represents the question of how the literature defines and conceptualizes ISA. This is important since a clear definition and coherent understanding of the topic is essential for valuable theoretical and practical investigations and implications. *Criterion 2* covers publications which explain and investigate the relationship between ISA and information security behavior. Having a closer look at the existing body of knowledge regarding this complex question can help to provide a better understanding of the motivational processes that transform an employee's ISA into desired behavior. *Criterion 3* focuses on potential antecedents of ISA. Understanding the factors that influence and optimally raise individuals' ISA provides valuable insights for security managers to enhance the effectiveness of their information security strategies. *Criterion 4* is abstracted to the term SETA programs (security, education, training, and awareness programs) – a collective term for all kinds of methods and tools used to educate, train and raise awareness of information security issues and to foster information security behavior among several stakeholders of an organization. The question of how SETA programs should be designed to be most effective is essential for security managers, since they certainly belong to the most important behavioral information security countermeasures of an organization. *Criterion 5* analyzes the common techniques and tools that researchers have deemed to be helpful in order to assess ISA levels of

individuals, employees, and organizations, and to ultimately make it measurable. Insights of this criterion can help security managers to identify the best fitting approach to evaluate the present state of employees' ISA, as well as to monitor the effectiveness of implemented ISA strategies.

After categorizing the literature into five main objectives of ISA research, the subsequent in-depth analysis – including a more detailed examination of the criteria and a discussion section revealing implications and research gaps – focuses on criterion 1, 2 and 3, whereas criterion 4 and 5 are excluded from this analysis for reasons that are explained within section 2.3 of the paper. The in-depth analysis of the literature encompasses three main research questions: (1) "how is ISA conceptualized and defined in the literature?" (2) "how does ISA relate to information security behavior?" and (3) "which factors influence ISA?".

The results of the analysis of criterion 1 show that there is a lack of a stringent accordance within the literature's conceptualization of ISA. Among the 131 selected publications, 21 different definitions of ISA are identified which cover three distinct perspectives of ISA, namely "cognitive", "behavioral", and "procedural". The results of criterion 2 reveal three dominant theories which are applied to explain the mechanisms that transform an individual's cognitive ISA into actual information security behavior – the general deterrence theory (GDT) (Gibbs 1975), the theory of planned behavior (TPB) (Ajzen 1985, Ajzen 1991), and the technology acceptance model (TAM) (Davis 1989). Deviated from these theories, five important mediating constructs through which ISA affects behavior indirectly are identified, namely IS-users' perceived severity and certainty that harmful information security behavior will be sanctioned, perceived usefulness and ease of use of information security technologies, and attitude towards information security. The analysis of criterion 3 identifies various antecedents of ISA, which can be assigned to three dimensions according to their level of origin, namely "individual", "institutional", and "socio-environmental". Most importantly, it becomes evident that there is an urgent need to conduct empirical studies examining suggested antecedents of ISA.

The second paper is allocated to criterion 3 of the classification scheme of the literature review and addresses the identified lack of studies which empirically investigate ISA's

antecedents. It proposes and tests a research model that incorporates different institutional, individual, and environmental antecedents of ISA. Moreover, it examines the important, yet not studied mediating role of ISA on the relationship between ISA's antecedents and employees' intention to comply with information security policies (ISPs). The model was tested with data obtained from 475 employees from a broad variety of organizations. The model explains a substantial proportion of the variance in ISA (R^2 = .50) and intention to comply with ISPs (R^2 = .40). The results support the theorized relationships indicating that the provision of security policies, SETA programs, employees' knowledge of information systems, negative experience with information security incidents, secondary sources' influence, and peer behavior are significant influencing factors of ISA. The results further indicate that ISA mediates the relationship between ISA's antecedents and behavioral intention. The findings provide important contributions for the body of knowledge of ISA research as well as for stakeholders who are interested in encouraging employees' information security behavior.

The third paper is allocated to criterion 2 of the classification scheme of the literature review. It develops and tests a model that expands our knowledge on the complex question of why some individuals are more highly motivated to comply with ISPs while others do not, and shows why deterrence – a principle that dominates the literature concerning this question – is not enough. The model integrates the theory of planned behavior (Ajzen 1985, Ajzen 1991), the organismic integration theory (Ryan and Connell 1989), and the concept of cognitive ISA (Bulgurcu et al. 2010). The guiding research questions include the influence of personal values, the role of external pressure and coercion, and the preceding role of endogenous motivation and attitude on the intention to comply. To empirically validate the model, data from a sample of 444 employees from different organizations were analyzed. The results show that, when employees' personal values and principles are congruent with their employer's information security related prescriptions and goals, their intention to comply with security policies significantly increases. On the contrary, no impact on compliance intention was found when employees perceive their actions as a result of external pressures and coercion. The model confirms the essential role of ISA for ISP compliant behavior by showing its preceding role for endogenous motivations, attitude, and the intention to comply. The study's findings advance our understanding of the motivational processes underlying

security compliant behavior and provide numerous implications for scholars and practitioners.

Study 2 and 3 both have been published in the conference proceedings of the International Conference of Information Systems (ICIS) which is one of the leading IS conferences worldwide. Table 1 shows a summarized overview of the three studies along with the research method, research questions, title, publication outlet, authors, and proportion of own contribution.

Overview of the Three Studies						
Study #	**Method**	**Research Questions**	**Title**	**Publication Outlet**	**Authors**	**Own Contri-bution**
I	Literature review	How is ISA conceptualized and defined in the literature? How does ISA relate to information security behavior? Which factors influence employees' level of ISA?	Information Security Awareness – A Review of the Literature: Definitions, Influence on Behavior, Antecedents	Will be submitted: Thirty Sixth International Conference on Information Systems (ICIS), Fort Worth, 2015	Haeussinger	100%
II	Empirical examination of a proposed causal model: quantitative field study	Which factors influence employees' level of ISA? What is the mediating role of ISA on the relationship between ISA's antecedents and employees' ISS behavior?	Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior	Accepted and published: Thirty Fourth International Conference on Information Systems (ICIS), Milan, 2013	Haeussinger and Kranz (2013)	80%
III	Empirical examination of a proposed causal model: quantitative field study	How do endogenous motivations and ISA influence individual ISS behavior?	Why Deterrence is Not Enough: The Role of Endogenous Motivations and Information Security Awareness on Employees' Information Security Behavior	Accepted and published: Thirty Fifth International Conference on Information Systems (ICIS), Auckland, 2014	Kranz and Haeussinger (2014)	80%

Table 1 Overview of the Three Studies

The remainder of this thesis is structured as follows. The following Chapter B. provides general background knowledge and definitions of the information security domain to give the reader a basic understanding of the topic before the actual three papers are outlined. The subsequent Chapters C, D., and E. contain the three papers. Each is self-contained and can be read separately. This approach involves a certain degree of redundancy between the papers. However, due to the studies' coherence and for reasons of clarity and comprehensibility, this cannot be completely avoided. Furthermore, it avoids referring back and forth between the chapters. Finally, the dissertation concludes with a brief summary of the studies' main theoretical and practical contributions and provides an outlook and directions for future research (Chapter F.).

B. General Background on Information Security

This chapter introduces the basic idea of organizational information security and provides the reader with a general understanding of the context in which the dissertation's topic of ISA research is embedded. It does not focus on ISA, but rather exemplifies general knowledge on the information security field, which is groundwork for the following three papers. The section begins by defining the terms of information security, information systems (IS), and information systems security (ISS). Subsequently, some key concepts and topics are introduced, such as the main goals of information security, existing threats, consequences and costs of information security, and the available countermeasures and controls. Furthermore, the section outlines the basic idea of information security management (ISM), and provides an overview of the ISM standards and best practice guidelines that exist in practice. Finally, the different types of information security behavior are introduced.

Information Security

There is a great variety of definitions of information security, which is often abbreviated to the term InfoSec. The international standard and code of practice for information security management ISO/IEC 27001 (2005, 2013) defines information security "… as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities." Information security is also defined, "… as a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats." (Cherdantseva and Hilton 2013, p. 546). Information security is a continuous process that involves people, policies, procedures, processes and technology (Rao and Nayak 2014). Accordingly, information security can be examined and executed from three interdependent layers, as illustrated in Figure 2.

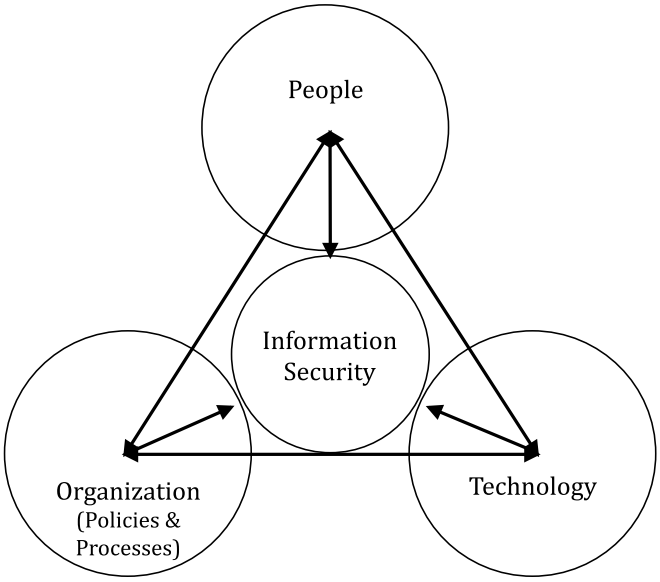


Figure 2: Layers of Information Security (Roa and Nayak 2014)

Information System

An information system (IS) is "…a socio-technical system, which delivers information and communication services required by an organization in order to achieve business objectives. In general an IS encompasses six components: (1) information and data, (2) people, (3) business processes, and information communication technologies (ICT), which include (4) hardware, (5) software, and (6) networks." (Cherdantseva and Hilton 2013, p. 547). An IS can also be simply defined as "… an aggregate of information handling activities at a technical, formal and informal level of an organization." (Liebenau and Backhouse 1990).

Information Systems Security

The literature often uses the terms information security and information systems security (ISS) synonymously. This is particularly the case if the definition of IS is not limited to the technical dimension of information handling activities, as defined above. This dissertation follows this perspective and does not distinguish between information security and ISS.

Information Security Goals (CIA Triad)

The basic information security concept states that there are three superior goals of information security, namely to ensure the confidentiality, integrity, and availability of information. The three goals are represented by the CIA triad, as presented in Figure 3 (ISO/IEC 27002 2005, 2013, Clinch 2009, Whitman and Mattord 2011).

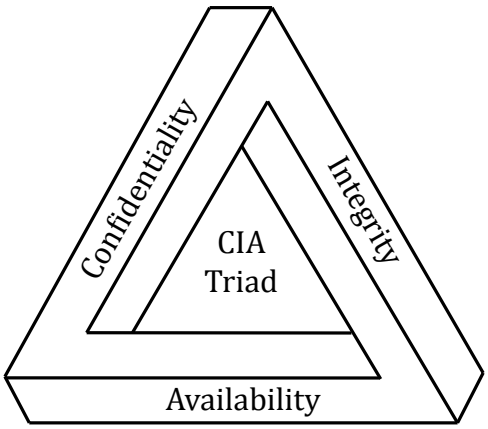


Figure 3: CIA Triad of Information Security

(1) Confidentiality: the assurance that only intended and authorized recipients or systems have access to information.
(2) Integrity: the assurance that information has not been changed or modified in storage or transmission except by authorized persons or processes.
(3) Availability: the assurance that information is available to authorized users or systems at the times they are authorized to access it.

The CIA triad was developed in the early beginnings of the computer era and has for several decades served as a popular conceptual model of ISS (Whitman and Mattord 2011, Cherdantseva and Hilton 2013). However, more recently the adequacy of the CIA triad as a complete set of ISS goals has been questioned, since it neglects new threats that emerge in the increasingly collaborative and de-perimeterized work environment (Parker 1998, Whitman and Mattord 2011, Cherdantseva and Hilton 2013). Cherdantseva and Hilton (2013) analyzed the extant information security literature to identify a more complete and currently relevant list of security goals, which extends the classic concept of the CIA triad. Table 2 illustrates this list, along with the goals' definitions and applicability to the six components of an IS.

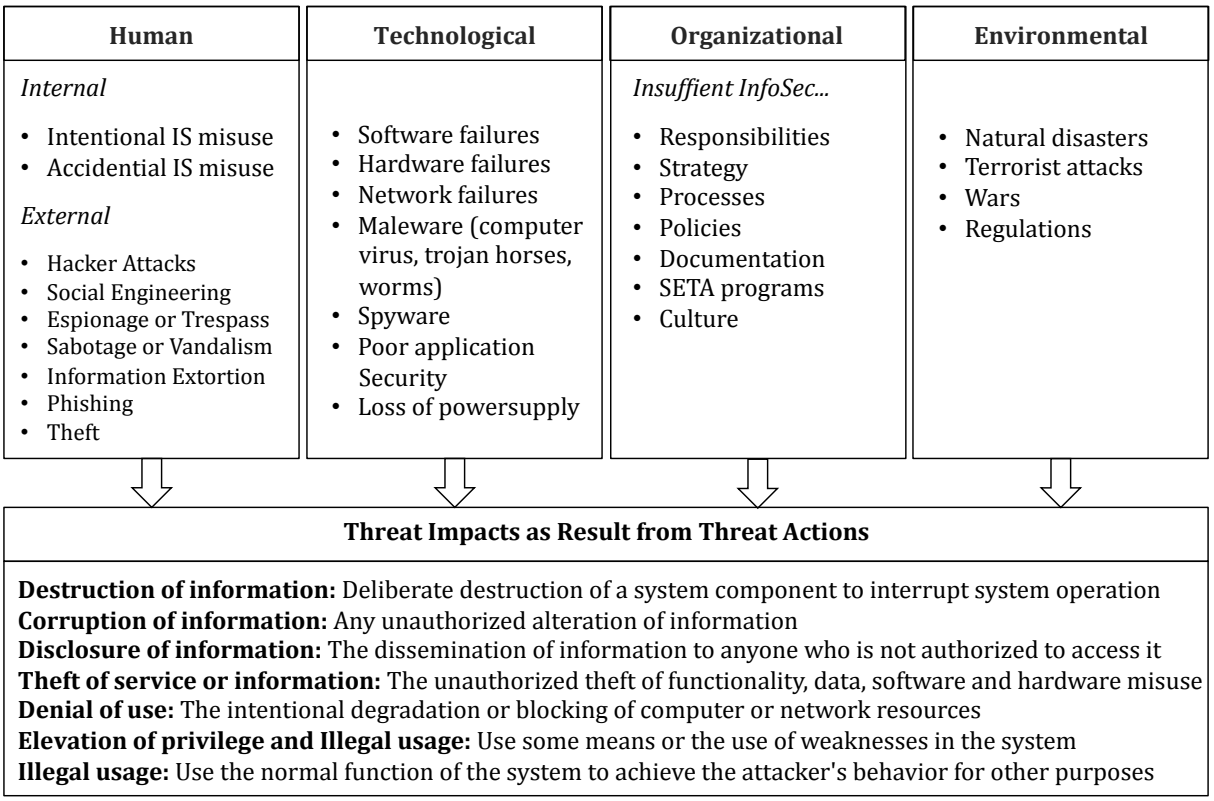
		Components of an Information System					
Information Security Goal	Definition	Information	People	Processes	Hardware	Software	Networks
Accountability	An ability of a system to hold users responsible for their actions (e.g. misuse of information)		x				
Auditability	An ability of a system to conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system			x			
Authenticity / Trustworthiness	An ability of a system to verify identity and establish trust in a third party and in information it provides	x	x	x	x	x	x
Availability	A system should ensure that all system's components are available and operational when they are required by authorized users	x	x	x	x	x	x
Confidentiality	A system should ensure that only authorized users access information	x					
Integrity	A system should ensure completeness, accuracy and absence of unauthorized modifications in all its components	x	x	x	x	x	x
Non-repudiation	An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event	x		x			
Privacy	A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user-involvement)	x	x				

Table 2: Information Security Goals (Cherdantseva and Hilton 2013)

Information Security Threats

Information security is all about ensuring business continuity and to minimize business risk by preventing and minimizing the impact of a wide range of threats (von Solms 1998, Kruger et al. 2010). In general, a threat can be defined as, "… a potential cause of an incident, that may result in harm of systems and organization." (ISO/IEC 27002 2005, 2013), or as, "…any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), information assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." (FIPS 200 2013). Threats are classified by various criteria in the literature. The most common criteria are source (internal/external), agent (human, technological,

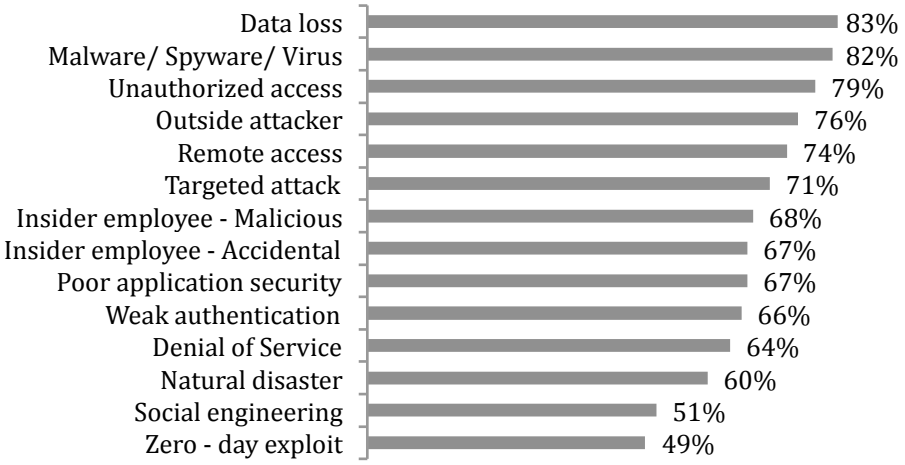
organizational, environmental), motivation (malicious or non malicious), and intention (intentional/accidental) (BSI 2014, Jouini et al. 2014). Threat impacts are direct harmful effects that result from threat actions, which are also often termed as information security incidents or security breaches (Jouini et al. 2014). Those impacts in turn affect the superior goals of information security as described above. Figure 4 shows an overview of the most common information security threats, classified according to the different threat agents (human, technological, organizational, environmental).



Note. The classification and examples are based on a detailed examination of Whitman (2003), BSI (2014), CSI (2010/2011), and Jouini et al. (2014). There is a vast amount of threats in the literature, this is by far not an exhaustive list of threats.

Figure 4: Classification of Information Security Threats

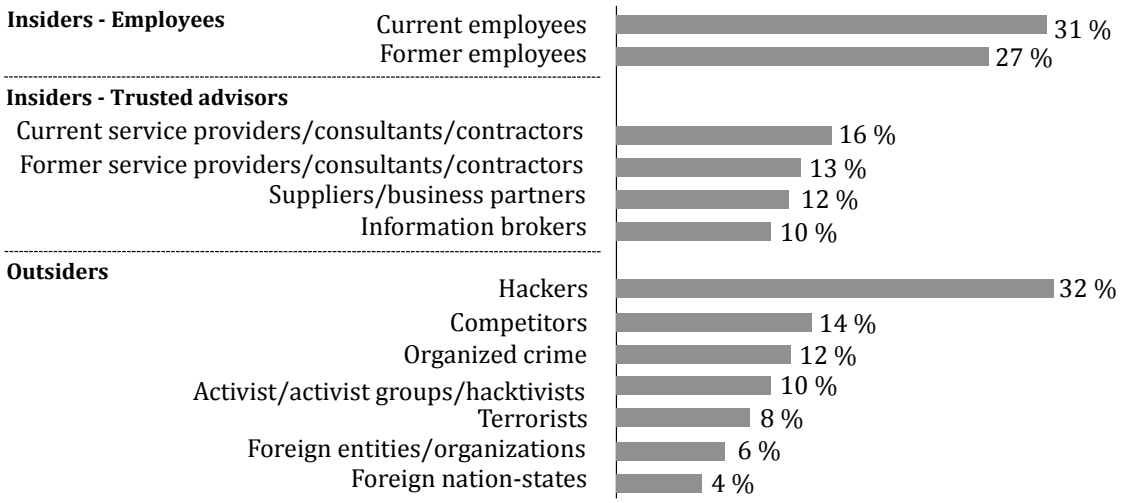
There is a broad landscape of information security threats which continues to grow and evolve. A survey conducted by the international research firm Evalueserve asked 495 organizations worldwide from a wide spectrum of industries (e.g., manufacturing, education, technology, government, healthcare, retail and financial services) to report the most important threats to their organization (McAfee 2012). Figure 5 shows the most frequent answers.



Note. Respondents were asked to state the most frequent information security threats. Multiple answers allowed. Not all factors are shown.

Figure 5: Frequent Information Security Threats (McAfee 2012)

Distinguishing between internal and external sources, the Global State of Information Security Survey (PWC 2014) reports the most common sources of threats as presented in Figure 6.



Note. Respondents were asked to state the most frequent information security threat sources. Multiple answers allowed. Not all factors are shown.

Figure 6: Sources of Information Security Incidents (PWC 2014)

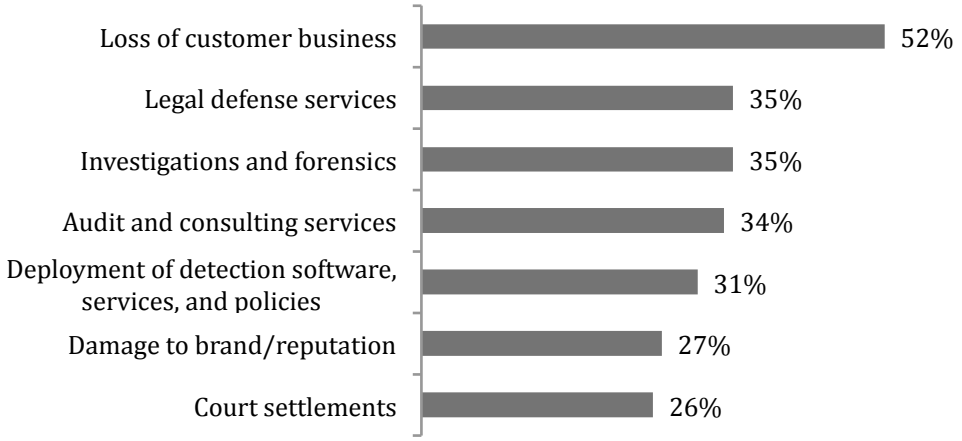
The dissertation's topic of ISA relates to the internal, human dimension of information security (see Figure 4). As illustrated above, threats from human agents are either external (e.g., hacker attacks) or internal (employees and trusted advisors and business partners). Indeed, it is assumed that 50 - 70 % of overall ISS incidents in organizations result either directly or indirectly from employees' behavior (Ernst and Young 2003, Siponen and Vance 2010). Internal human threats caused by employees range from naïve mistakes to intentional harm, or in other words are either accidental or intentional. Intentional threats are the result of a harmful decision, such as computer crimes including espionage, identity theft, purposely damaging property or stealing customers' credit card information (Jouini et al. 2014). Unintentional threats are caused by low ISA, and include the unauthorized or accidental violations of information security caused by programming and user or operator behavioral error (Jouini et al. 2014). Avoiding employees' human error is the main focus of ISA research.

Cost of Information Security

The Global State of Security Survey surveyed more than 9,700 security, IT, and business executives and found that the total number of security incidents (threat actions) reported by the respondents climbed to 42.8 million events in 2014 – an increase of 48% over 2013 (PWC 2014). In the long run the survey data shows that the compound annual growth rate (CAGR) of reported security incidents has increased 66% year-over-year since 2009. A recent study in the UK has shown that the average cost of a single internally caused security incident was between £1 million and £2 million for very large organizations (Chen et al. 2012b). The Centre for Strategic and International Studies (CSIS) estimates the global costs of information security incidents and cyber crime in organizations to be approximately $445 billion each year (The Economist 2014).

In general, the damages caused by information security incidents occur in the form of explicit and implicit costs (Gordon et al. 2011). The explicit costs represent the costs of finding and correcting the sources of a threat, while the implicit costs describe the loss of future transactions caused by the intrusion in both the relationships between a company and its customers and a company and its business partners (Gordon et al. 2011). The indirect effect of a security breach can go as far as it negatively influencing the market value of a company (Cavusoglu et al. 2004). In addition, organizations

struggle with legal and regulatory problems, bad publicity or governmental sanctions that result from harmful ISS incidents (Goel and Shawky 2009, Siponen et al. 2009). Figure 7 shows some of the most frequently reported reasons for financial losses from security breaches.



Note. Respondents were asked to state the most frequent sources of financial loss. Multiple answers allowed. Not all factors shown.

Figure 7: Sources of Financial Loss (PWC 2013)

Information Security Countermeasures

According to the research firm Gartner, organizations around the world reportedly spent more than $ 67 billion in 2014 to defend themselves from information security threats, and the expenditures are expected to grow to $86 billion in 2016 (The Economist 2014). To achieve ISS, organizations typically implement a suitable set of controls and countermeasures (ISO/IEC 27002 2005, 2013). Security countermeasures are ways to detect, prevent, or minimize losses associated with information security threats (Peltier 2001, Yeh and Chang 2007). Former attempts to ensure ISS have focused on technical countermeasures, which typically referred to assets such as hardware, software and networking systems (Stanton et al. 2005, Spears and Barki 2010). In trying to achieve technological integrity with ISS, companies introduced the use of passwords, firewalls, anti-virus software, or backup systems. However, several studies have revealed that technical countermeasures alone are not sufficient to address the various types of information security issues, and that a more comprehensive approach to security is required, meaning that countermeasures of a different nature should be exploited (Winkler and Dealy 1995, Cherdantseva and Hilton 2013). In this regard,

organizations introduced behavioral control and management instruments, such as information security policies (ISPs), security education training and awareness (SETA) programs, and sanctions and rewards to complement their technological security efforts and to address the human dimension of ISS (Chen et al. 2012b). The British security standard and guidance for best information security management practices BS 7799-2 (2002) code proposes a set of more than 100 security controls in 10 different categories (Yeh and Chang 2007). It is beyond the scope of this chapter to exemplify the detailed taxonomies of security controls. However, at a higher level of abstraction, Cherdantseva and Hilton (2013) classify the available set of security countermeasures into four dimensions, namely organizational, technical, human-oriented, and legal. Figure 8 shows this classification, along with a list of the most common examples.

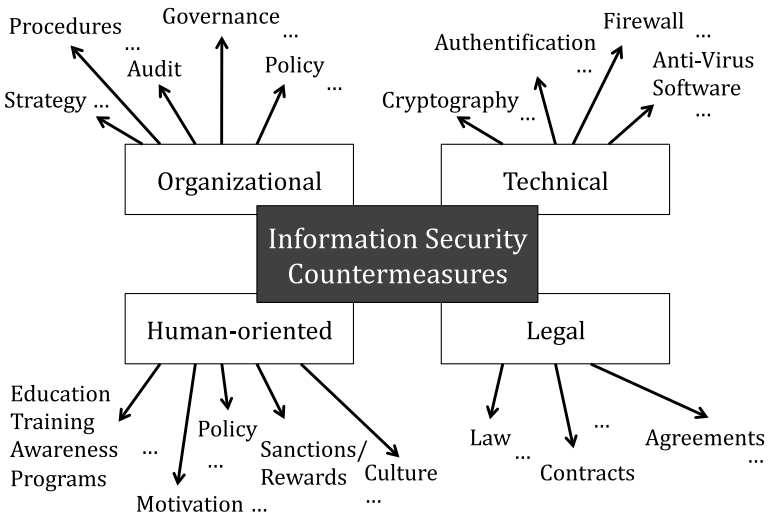


Figure 8: Information Security Countermeasures (Cherdantseva and Hilton 2013)

Information Security Management

The goal of information security management (ISM) is to ensure the confidentiality, integrity and availability of an organization's assets, information, data and IT services through proactive management of information security risks, threats and countermeasures (Kritzinger and Smith 2008, Clinch 2009). ISM is also defined as "… a systematic process of effectively coping with information security threats and risks in an organization, through the application of a suitable range of physical, technical or

operational security controls, to protect information assets and achieve business goals (Tu and Yuan 2014). ISM is a business function, which is primarily concerned with strategic, tactical, and operational issues of the planning, analysis, design, implementation, and maintenance of organizational information security (Choobineh et al. 2007, Tu and Yuan 2014). According to Vermeulen and von Solms (2002), ISM activities cover a) preparation elements (e.g. gain top management commitment, describe security vision and strategy), b) implementation elements (e.g. determine security requirements, formulate security policy, perform risk management, implement safeguards and procedures), and c) maintenance or continuation elements (e.g. monitor security situation, ensure proper incident handling) (Tsohou et al. 2010).

Information Security Management Standards

In practice there are different international security standards available which attempt to provide best practices for ISM. These guidelines play a key role in managing organizational ISS. By complying with a set of rules and practices proposed by such authoritative guidelines, organizations can demonstrate their commitment to ISS practices and may apply for certification, accreditation, or a security-maturity classification (Siponen and Willison 2009). Exemplifying the broad field of ISM standards and best practices in more depth is outside the scope of this chapter. However, Table 3 provides an overview of the most popular standards, along with a brief description.

The most widely accepted ISM standards are ISO/IEC 27001 (2005, 2013) and ISO/IEC 27002 (2005, 2013), since they offer the most comprehensive approach to ISM, whereas the other standards focus more on IT governance, in general, or on the technical aspects of ISS (Saint-Germain 2005, Tsohou et al. 2010). The ISO standards provide a baseline set of controls which cover the places, people, and process requirements that organizations need in order to provide suppliers, staff, and customers with confidence in its information security (Qudaih et al. 2014). They describe ISM as the development, implementation, and maintenance of an information security management system (ISMS) which is structured into four phases, plan, do, check, and act, as presented and described in Table 4 (Tsohou et al. 2009).

ISM Standards and Best Practices	Description/Scope	Offers Certification?
ISO/IEC 27001 (2005, 2013)	ISO/IEC 27001 is an international standard that specifies an ISM system (ISMS) which provides a set of controls covering the places, people, and process requirements that organizations need in order to provide ISS. This is the top-level specification and certification standard for effective ISM for all types of organizations.	Yes
ISO/IEC 27002 (2005, 2013)	ISO/IEC 27002 is usually used beside ISO/IEC 27001 standards. It establishes further practical guidelines and best practices for initiating, implementing, maintaining, and improving ISM in an organization. Thereby it relies on risk assessment and treatment principles.	Yes
COBIT (Control Objectives for Information and (Related) Technology)	COBIT is an international standard for IT governance that seeks to bring together business control models and IT control models.	No
ITIL (Information Technology Infrastructure Library)	A supplement to committee COBIT that proposes best practices for IT service management.	No
CERT Security Practices	A set of recommended best practices for improving the security of computer network systems.	No
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	An assessment and planning framework for security that enables companies to identify and analyze risks and develop a plan to mitigate those risks.	No
SSE-CMM (System Security Engineering Capability Maturity Model)	A model for assessing the security maturity level of an organization. Five security levels exist, from 1 (performed informally) to 5 (continuously improving). SSE-CMM does not describe a way of doing things but rather reports widespread practice.	No
GMITS (Guidelines for the Management of IT Security)	GMIS is an international standard that lays out guidelines for information security management and consists of a number of technical reports covering information security management concepts and models, techniques, IT security management and planning, and selection of safeguards.	No
Common Criteria for Information Technology Security Evaluation (ISO 15408)	A technical standard that certifies the levels of defense conferred by the security measures implemented in information systems	Yes
ISF (2007) (Information Security Forum)	Is a standard of good practice which addresses ISS from a business perspective, providing a practical basis for assessing an organization's ISS arrangements.	No
NIST (2003, 2006) (National Institute of Standards and Technology)	Provides a holistic step-by-step management guide for executing the process (development, implementation, post-implementation) of effective information security awareness (ISA) programs.	No
ENISA (2008) (European Network and Information Security Agency)	Provides a holistic management guideline for planning and executing effective security, education, training, and awareness (SETA) programs.	No

Table 3: ISM Standards and Best Practices (Saint-Germain 2005)

PDCA Phase	Description
Plan (establish the ISMS)	• Define the ISMS scope and the organization's security policies • Identify and assess risks • Select control objectives and controls that will help manage these risks • Prepare the Statement of Applicability documenting the controls selected and justifying any decisions not to implement, or to only partially implement, certain controls
Do (implement and operate the ISMS)	• Formulate and implement a risk mitigation plan • Implement the previously selected controls to meet the control objectives
Check (monitor and review the ISMS)	• Conduct periodic reviews to verify the effectiveness of the ISMS • Review the levels of acceptable and residual risk • Periodically conduct internal ISMS audits
Act (maintain and improve the ISMS)	• Implement identified ISMS improvements • Take appropriate corrective and preventative action • Maintain communication with all stakeholders • Validate improvements

Table 4: PDCA Model of an ISMS (ISO/IEC 27001 (2005, 2013) (Saint-Germain 2005)

ISO/IEC 27001 (2005, 2013) are the only comprehensive best practice frameworks that allow organizations to undergo a third-party audit and become certified (Saint-Germain 2005). 11 ISM topics are covered in total, for which the standards suggest security control clauses. These collectively contain a total of 39 main security categories and one introductory clause introducing risk assessment and treatment. The 11 main domains are:

(1) Security Policy

(2) Organizing Information Security

(3) Asset Management

(4) Human Resources Security

(5) Physical and Environmental Security

(6) Communications and Operations Management

(7) Access Control

(8) Information Systems Acquisition, Development and Maintenance

(9) Information Security Incident Management

(10) Business Continuity Management

(11) Compliance

Information Security Behavior

This dissertation's topic of ISA is an important part of the behavioral stream of ISS research, which focuses on the human dimension of information security. Parts of information security behavior were already introduced in the section on information security threats (see internal human threats in Figure 4). However, information security behavior, also referred to as ISS behavior within this dissertation, is a broader term, and includes not only threatening security behaviors, but also positive and desired security practices conducted by well-trained and aware end users. In the literature, ISS behavior is often simply defined as users' compliance or non-compliance with their organization's security policy (Siponen et al. 2009, Jenkins et al. 2011). In a less abstract view, Stanton et al. (2005) classify a taxonomy of six different behavior types using intentionality and technical expertise as criteria. They name them intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance, and basic hygiene. Figure 9 shows the two-factor taxonomy of end user security behaviors. Table 5 outlines the corresponding descriptions and examples of each behavior type.

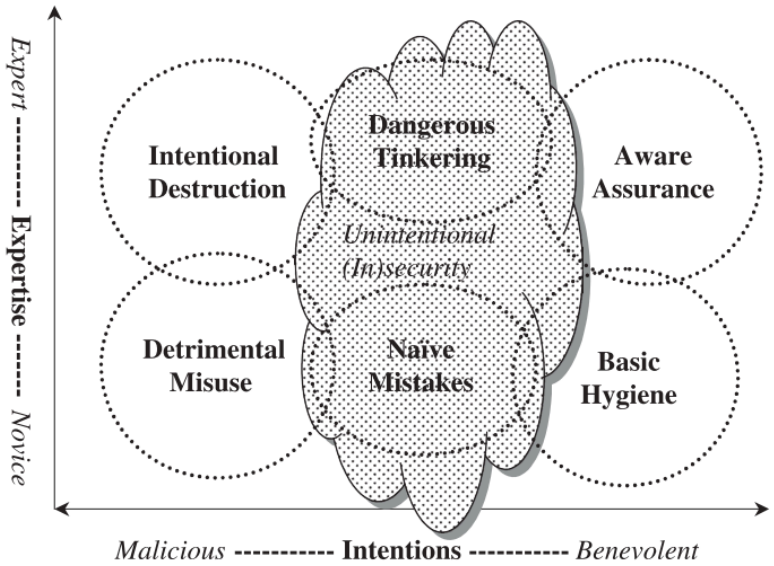


Figure 9: Two-Factor Taxonomy of End User Security Behaviors (Stanton et al. 2005)

Expertise	Intentions	Title	Description
High	Malicious	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret.
Low	Malicious	Detrimental misuse	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources. Example: choosing a bad password such as ''password.''
High	Beneficial	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

Table 5: Two-Factor Taxonomy of Security Behaviors (Stanton et al. 2005)

This chapter exemplified the basic idea of organizational ISS with the aim to provide the reader with a general understanding of the context in which the dissertation's topic of ISA research is embedded. In the subsequent sections, the three studies of the dissertation are outlined.

C. Study I: Information Security Awareness – A Review of the Literature: Definitions, Influence on Behavior, Antecedents

Abstract

Living in a digital age, where all kinds of information are accessible electronically at all times, organizations worldwide struggle to keep their information assets secure. It is assumed that 50 - 70 % of overall information systems security (ISS) incidents in organizations are either directly or indirectly the result of human error (Ernst and Young 2003, Siponen and Vance 2010). In order to explore how organizations can defend themselves against the harmful ISS behavior of their employees, the topic of information security awareness (ISA) has become a top priority in the community. Hitherto existing ISA literature, however, lacks a coherent understanding of the subject and is not well structured. This study addresses these shortages and provides an extensive review of the literature on employees' ISA with the aim to provide quick structured access to the accumulated knowledge of ISA research, to give implications for scholars and practitioners and to reveal potential areas for further research (Webster and Watson 2002). 131 ISA publications are identified in a broad variety of information systems journals (e.g., MIS Quarterly, Information Systems Research), specific ISS journals (e.g., Computers & Security, Information Systems Security Journal), and conference proceedings (e.g., ICIS, ECIS, AMCIS). By applying an open coding technique based on grounded theory (Strauss and Corbin 1990) a classification scheme is developed that graduates five main objectives of ISA research. The subsequent in-depth analysis follows this classification scheme and focuses on three research questions: (1) "how is ISA conceptualized and defined in the literature?", (2) "how does ISA relate to information security behavior?", and (3) "which factors influence ISA?". Providing this literature review hopefully leads to a better and unambiguous comprehension of the topic, provides a quick accessible starting point for scholars, and ultimately reveals the need for further research. Findings might also be useful for organizations' security managers to master the challenge of achieving high levels of ISA and compliant behavior of all kinds of stakeholders.

1 Introduction

Information systems security (ISS) is an increasingly critical issue for companies worldwide. In 2013, cybercrime and intellectual-property theft was estimated to have caused losses worth US $445 billion – a sum that roughly equals the GDP of a relatively small but wealthy European country, such as Austria (The Economist 2014). Besides criminal attacks and system malfunctions, human error is the major reason for information security incidents. Employees' ISA has been identified as one of the behavioral key factors in contributing to a successful ISS strategy (Siponen 2000, Dinev and Hu 2007, D'Arcy et al. 2009, Bulgurcu et al. 2010). Studies argue that the lack of employees' ISA of security policies and best practices is a major cause for ISS misbehavior and its consequences (Thomson and Solms 1998, Siponen 2000, Abraham 2011). In accordance with the community's growing attention to ISA, a considerable body of literature has evolved. Nevertheless, the number of publications dealing with ISA still can be considered as small in relation to the relevance of the topic (Rezgui and Marks 2008).

ISA is most frequently referred to as a cognitive state of mind, which is characterized by recognizing the importance of information security and being aware and conscious about ISS objectives, risks and threats, and having an interest in acquiring the required knowledge to use IS responsibly (Straub and Welke 1998, Thomson and von Solms 1998, Siponen 2000). However, delving deeper into the multitude of publications reveals that no universal understanding of ISA exists. Various studies claim to deal with ISA but indeed focus on ISS behavior (e.g. compliance with ISS guidelines, IS misuse, etc.) (e.g., Siponen 2000, ISF 2007, Hellqvist et al. 2013, Lebek et al. 2013a and 2014) or even equate the term ISA with organizational awareness-raising programs (Peltier 2005, Rastogi and von Solms 2012). In addition, prior literature reviews neglect this distinction and largely focus on behavior (Puhakainen 2006, Lebek et al. 2013a, 2014) or on security awareness strategies, campaigns, and programs (e.g. Puhakainen and Siponen 2010, Karjalainen and Siponen 2011), or are not up-to date and of unsatisfying coverage (e.g., Tsohou et al. 2008). However, it is essential to clearly distinguish ISA from behavior and awareness programs, since one can be aware of ISS issues and attend several security education, training, and awareness (SETA) programs, but still fail to

comply with the employer's information security policies (ISPs) (Siponen 2000). Beyond that, the literature is multifaceted, diffuse and lacks structure. There is a need to review the literature following the perspective that ISA does not equal behavior, to discover potential areas for further research, and to bring structure into this important field. This study aims to fill these gaps and provides a synthesized up-to-date review of the current state of ISA literature by addressing three essential research questions (RQ). These have been chosen because they are deemed to be most important for scholars and practitioners and, furthermore, provide the groundwork for the subsequent empirical studies in this dissertation:

RQ1: How is ISA conceptualized and defined in the literature?

RQ2: How does ISA influence ISS behavior?

RQ3: Which factors precede employee's ISA?

Reviewing and analyzing the ISA literature is useful for researchers and practitioners, since it provides systematic and quick access to the aggregated knowledge of the topic, discovers existing objections and deficits, and reveals gaps for further research (Abraham 2011). Findings can help organizations' security managers to improve the effectiveness of awareness raising programs, increase employees' ISA and ultimately foster their policy compliant behavior.

The remainder of the study is organized as follows. In the next section, the methodology used in the review is exemplified. This includes the identification and selection process of the relevant publications, the applied method, as well as the introduction of the classification scheme. In section three the literature is reviewed and analyzed in more depth according to the three research questions. In the last section the findings are critically discussed, theoretical and practical implications are given, and gaps for future research, as well as the study's limitations are outlined.

2 Methodology

In the following, the procedure of identifying and selecting the relevant literature is illuminated. Subsequently, the methodological approach used and the development of the classification scheme of the literature are exemplified.

2.1 Identification Process of Relevant Literature

The quality of a literature review strongly depends on the search process (Brocke et al. 2009, Lebek et al. 2013a, 2014). To identify the relevant publications for this review, the structured approach for gathering literature proposed by Webster and Watson (2002) is applied. According to the guidelines from Brocke et al. 2009, a rigorous literature search must fulfill the premise of validity and reliability. Validity with regard to a literature search, represents the degree to which the search process accurately uncovers the sources that the reviewer is intending to collect (Brocke et. al 2009, Lebek et al. 2013a, 2014). This is fulfilled within this review by the selected databases, journals, publications, used keywords and an additional forward and backward search. To fulfill the requirements of "reliability", the literature search process must be replicable (Brocke et al. 2009). This is achieved by the detailed documentation of the search process. To avoid limitations due to a small sample of journals, it was the aim to search not only the top reputational IS journals, but also specialized journals from the information security field, conference proceedings, surveys, and doctoral dissertations. Non peer-reviewed publications such as books and working papers, in common with doctoral dissertations, which are not accessible to the broad public, were excluded. Furthermore, the search was limited to publications written in the English language.

Keywords	
Information security awareness	Antecedents of information security awareness
IT security awareness	Assessment of information security awareness
Security awareness	Information security awareness program
Information security awareness management	Information security awareness campaign
Employees' information security awareness	Information security behavior
Definition of information security awareness	Information security policy compliance

Table 6: Utilized Keywords for the Literature Search

Following Webster and Watson (2002), the structured search process began with a keyword search using a list of pre-defined search terms on ISA (see Table 6) in the major IS journals ("A" in Table 7). Subsequently, the keyword search was conducted in the leading academic literature databases ("B" in Table 7) to cover the majority of other relevant journals and conference proceedings. As a last step in the keyword search, a "Google Scholar" search with the abovementioned search terms was consulted to find research work that was not covered by these databases. In addition to the keyword search, selected journals and conference proceedings' tables of contents ("D" and "E" in Table 7) were screened to pinpoint articles that were not covered by the keyword search. After the keyword search, a backward search was conducted reviewing the citations of the articles identified and extracting those dealing with ISA issues which were not found during the first step. Finally, the Web of Science (the electronic version of the Social Sciences Citation lndex) was used to identify articles that cited some of the key articles in the previous steps and included the relevant ones into the analyses. This first literature identification process in total revealed 427 potentially relevant publications.

Search Sources	
A) Major IS journals	**D) Specialized Information Security Journals**
Information Systems Research	Computers & Education
MIS Quarterly	Computers & Security
Journal of Management IS	Computer Fraud & Security
Information Systems Journal	International Journal of Computer Science and Information Security
	Information Management & Computer Security
B) Leading academic databases	Information Systems Security Journal
Emerald Library	
EBSCO	**E) Conference proceedings**
Elsevier Science Direct	American Conference on Information Systems (AMCIS)
ACM Digital Library	European Conference on Information Systems (ECIS)
EconLit	International Conference on Information Systems (ICIS)
IEEE Electronic Library	IFIP TC11 International Conf. on Information Security (IFIP TC11)
	International Conf. on Security of Information and Networks (SIN)
C) Other tools	First World Conference on Information Security Education (WISE)
Google Scholar	Annual ACM SIGUCCS conference on User Services (SIGUCCS)
Web of Science	Hawaii International Conference on System Sciences (HICSS)

Table 7: Sources of the Literature Identification Process

In the next step the 427 publications' titles, abstracts, and, if necessary, full texts were screened to filter out those publications which did not deal directly with ISA issues but were identified through the applied keyword search described above. Furthermore, based on a subjective evaluation, ISA publications which were not relevant and of small value for this review were also excluded, just as articles which focused on very specific ISA issues and which therefore were out of scope of this review. Publications before the year 2000 were only included if they were deemed to represent important groundwork (e.g., Straub and Welke 1998, Thomson and von Solms 1998), since the aim is to provide an up-to-date review of the research field. Although the focus of this survey is the organizational context, articles that deal with other contexts, such as "home Internet users" or "student IS-users" were included, since those may also provide valuable insights into the topic. Taking the previous identification and selection steps into account, the final sample of publications consists of 131 relevant articles.

2.2 Methodological Approach

This literature review is of an explorative nature and applies open coding technique based on grounded theory (Glaser and Strauss 1967, Strauss and Corbin 1990). Grounded theory coding is a kind of qualitative content analysis to find, categorize and conceptualize core issues from within a huge pile of data. Open coding means systematically breaking down data into separate units and categories to abstract different properties and dimensions of a corresponding topic (Strauss and Corbin 1990). Open coding also allows one to be guided by a set of pre-defined questions and directions before becoming selective (Moghaddam 2006). This was done by the three research questions RQ1, RQ2, and RQ3, as outlined in Chapter 1.

2.3 Classification Scheme

The open coding process revealed that the ISA domain can be divided into five main categories, each of which represents a different issue of concern of ISA research (see Figure 10).

First of all, ISA needs to be clearly defined, since a coherent understanding of the topic is essential for valuable theoretical and practical investigations and implications. Accordingly, this study has a closer look at how literature perceives and defines ISA

(criterion 1). The second cluster of literature addresses aspects concerning the relationship between ISA and ISS behavior *(criterion 2)*. This is important, since it is the ultimate goal to avoid ISS misbehavior and to foster proper ISS behavior. Having a closer look at how this relationship has been explained and explored can help to provide a better understanding of the motivational processes that underlie an employee's ISS performance. The third category of ISA research focuses on potential antecedents of ISA *(criterion 3).* Since ISA is a fundamental prerequisite of ISS behavior, understanding the factors that influence and optimally raise individuals' ISA provides valuable insights for security managers to help them enhance the effectiveness of their ISS strategies. The fourth cluster can be abstracted to the term security education training and awareness (SETA) programs, which is a collective term for all kinds of methods and tools used to educate, train and raise awareness of ISS issues among several stakeholders of an organization *(criterion 4).* Studies of this category investigate a broad variety of approaches, methods, contents, and success factors of SETA programs, and try to find out how these programs should be designed to be most effective for increasing employees' ISA levels and ISS behavior. SETA programs certainly belong to the most essential behavioral ISS countermeasures of an organization. The fifth and last cluster is dedicated to investigate techniques and tools to assess and evaluate ISA levels of individuals, employees, and organizations, and ultimately make it measurable *(criterion 5).* Analyzing the common techniques that researchers have deemed to be helpful in order to assess ISA levels helps security managers to identify the best fitting approach to assess the present state of employees' ISA, as well as to monitor the effectiveness of implemented SETA programs.

As mentioned before, the subsequent in-depth analysis of the literature focuses on criterion 1, 2, and 3. This is for two reasons. First, there already exist academic literature reviews that especially examine the extant literature dealing with SETA program approaches and the question of how these programs should be designed, implemented and executed to optimize their effectiveness (criterion 4) (Puhakainen 2006, Puhakainen and Siponen 2010, Karjalainen and Siponen 2011). Thus, analyzing the body of literature with regard to criterion 4 would be redundant with former literature reviews, and is, furthermore, out of the scope of this paper. Second, the focus is on those facets of ISA research, which are essential for the following empirical papers of this

dissertation. These are dedicated to an empirical examination of potential antecedents of ISA on the one hand (criterion 3) and on motivational processes that transform ISA into behavior (criterion 2) on the other hand.

Since valuable information was gathered during the comprehensive screening and open coding process with regard to criterion 4 and 5, tables are inserted which provide the key issues of the articles as well as a logical categorization into further sub-dimensions of criterion 4 in Appendix 2 – 7, and of criterion 5 in Appendix 8.

The following Figure 10 illustrates the classification scheme of the ISA literature. The final set of 131 identified ISA publications organized in alphabetical order of the authors along with the correlation with the five criteria of the classification scheme can be found in Appendix 1.

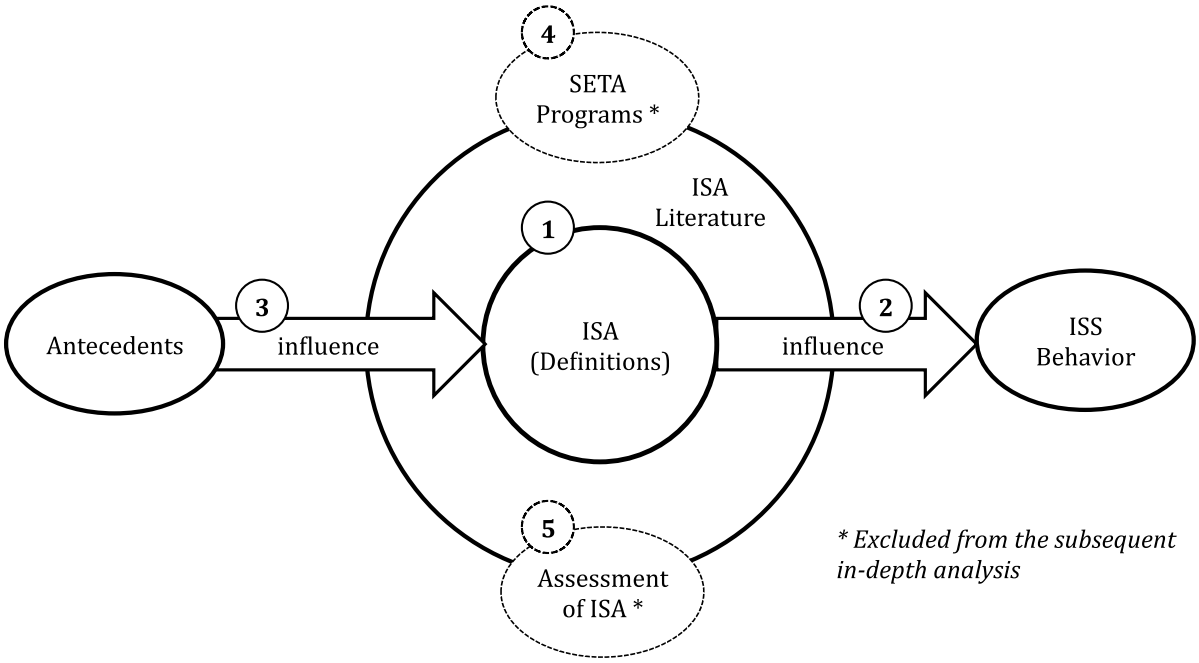


Figure 10: Classification Scheme of ISA Literature

3 Review

In the forthcoming sections, the findings of the in-depth analysis of the literature review regarding criteria 1, 2 and 3 of the classification scheme are illustrated. By having a closer look at the three fields, each is broken down into a subset of categories to get a better and more profound understanding of the literature, and ultimately provide scholars and practitioners with a detailed and structured access to the accumulated knowledge provided by these studies (Webster and Watson 2002). This analysis is again guided by open coding principles as explained in Section 2.2.

3.1 Definitions of Information Security Awareness

The term "awareness" itself is within its limits vague and can bear different meanings depending on the interpreter. As most people would understand it, the basic interpretation of awareness means something that happens in one's mind, paying attention to certain issues, knowing about and understanding certain things. Similarly, the Chambers 21st Century Dictionary specifies awareness and being aware in the following way:

- “awareness - noun: the fact or state of being aware, or conscious, especially of matters that are particularly relevant or topical”
- “aware - adj: 1. (often aware of something or someone) acquainted with or mindful of it or them. 2. (aware that ...) conscious that ... 3. well informed.”

By analyzing the term awareness with regard to ISS literature, it became evident that there exists no one universal definition. This might largely be due to ISA’s informal and socially constructed nature (Tsohou et al. 2008). Within the 131 analyzed articles, 21 more or less distinctive definitions of the term ISA are identified. It is noticeable that the number of articles clearly and explicitly defining ISA is surprisingly few. The majority of literature does not define the topic at all, although it is the main object of its research. However, further 17 studies are found that define ISA explicitly by following one of the 21 definitions.

By having a closer look at the definitions, it became obvious that ISA is not solely represented by a cognitive state of mind (e.g., being conscious and aware of information

security issues), as one would expect. There are several authors who do not distinguish awareness from behavior, and some who even mean awareness raising activities and the process of making individuals aware when talking about ISA. Accordingly, although a large variety of definitions exists, the open coding process resulted in three main aspects of literature's understanding of the topic, namely "cognitive", "behavioral", and "process". How each perspective is characterized will be exemplified in more detail in the subsequent sections. Some definitions cover only one aspect, others two or all of them. A summary of all identified ISA definitions along with the allocation of the three aspects "cognitive", "behavioral", and "process" is illustrated in the following Table 8.

Definitions of ISA (1 of 3)					
Author	**Explicit Definition**	**Cognitive Aspects**	**Behavioral Aspects**	**Process Aspects**	**Applied by**
Banerjee and Pandey (2010), Banerjee et al. (2013)	"Security awareness can be defined as the knowledge that members of an organization possess regarding protection of the physical and information assets of that organization."	x			
Bray (2002)	"Security awareness is a training effort designed to raise the security consciousness of employees."	x		x	
Bulgurcu et al. (2009, 2010)	"General information security awareness (GISA) and information security policy awareness (ISPA) are the key dimensions of information security awareness. GISA is defined as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications. ISPA is defined as an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements."	x			Al-Omari et al. (2011, 2012), Chan and Mumbarak (2012)
Choi et al. (2006, 2008)	„ ... the term "managerial information security awareness" in the current study starts from being aware of the significance of information security."	x			
D'Arcy and Hovav (2007a, 2007b, 2008), D'Arcy et al. (2009)	"IS-users' awareness of security countermeasures: awareness of security-policy statements and guidelines, SETA Programs, and computer monitoring."	x			Al-Omari et al. (2011, 2012)

Definitions of ISA (2 of 3)					
Author	**Explicit Definition**	**Cognitive Aspects**	**Behavioral Aspects**	**Process Aspects**	**Applied by**
Dinev and Hu (2007), Dinev et al. (2009)	"... define technology awareness as the users following and being interested in and knowledgeable about technological issues, problems and strategies to solve them."	x	x		
Galvez and Guzman (2009)	"... we define ISA as user's increased consciousness of and interest in knowing about security issues and the strategies to deal with them. ISA is one of the information security behaviors."	x	x		
Hellqvist et al. (2013)	"Security awareness is thus about understanding the information security policies, as well as complying with them."	x	x		
ISF (2007)	"Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly."	x	x		Albrechtsen (2007), Khan et al. (2011), Kruger and Kearney (2006), Wipaway-angkool (2009a,b)
Kritzinger and Smith (2008)	"Information security awareness is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with."	x		x	
Lim et al. (2010)	"Security awareness are programs that teach employees to be conscious about information security policies and procedures."	x		x	
NIST (2003)	„ The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly."; "…awareness seeks to focus an individual's attention on an issue or set of issues."	x	x	x	Al-Hamandi (2006), Chen et al. (2006), ENISA (2006), Okenyi and Owen 2007)
Peltier (2005)	"Awareness, which is used to stimulate, motivate, and remind the audience what is expected of them."			x	
Rastogi and von Solms (2012)	"Information security awareness is a vital communication tool used by organizations to influence end-users towards compliance with information security policies and controls in the organization."			x	

Definitions of ISA (3 of 3)					
Author	**Explicit Definition**	**Cognitive Aspects**	**Behavioral Aspects**	**Process Aspects**	**Applied by**
Rotvold and Braathen (2008)	"Security awareness is the extent to which every member of an organization and every other individual who potentially has access to the organization's information understand: Security and the levels of security appropriate to the organization; The importance of security and consequences of a lack of security; Their individual responsibilities regarding security, and act accordingly."	x	x		
Shaw et al. (2009)	"Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks."	x	x		
Siponen (2000)	"The term "information security awareness" is used to refer to a state where users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines)."	x	x		Heikka (2008), Mancha and Dietrich (2007), NG and Kankan-halli (2008), Siponen (2001), Rezgui and Marks (2008)
Spears and Barki (2010)	"Organizational information security awareness refers to different target groups (e.g., end users, IS professionals, senior management, third parties, etc.) (Siponen 2001), that exhibit a consciousness about organizational policies, procedures, or the need to protect sensitive information."	x			
Spurling (1995)	"When we talk about promoting computer security awareness and building commitment to computer security, we tend to think about security awareness campaigns, advertising, videos, posters, stickers, booklets, etc. All these things are important and have their place in promoting awareness, but in reality they are only part of the whole process."			x	
Tsohou et al. (2009)	"Awareness is an interfunctional process (check, act, plan, do) that crosses different divisional units or departments of organizations."			x	

Table 8: Definitions of ISA

3.1.1 Cognitive Perspective

Most frequently, ISA's definition is based on the "cognitive perspective". From this point of view, ISA is defined as an employee's state of mind, which is characterized by recognizing and understanding the importance and significance of ISS, being aware and conscious about ISS objectives, risks and threats, and having the required knowledge to use IS responsibly. One of the most often used and cited definitions of this stream has been provided by Siponen (2000), who refers to ISA as, "… a state where IS-users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines)". Although this definition largely represents the cognitive perspective, it also incorporates a behavioral aspect, since "being committed to the security mission" implies that one follows the prescribed rules of that mission. The definition by Bulgurcu et al. (2009, 2010) provides a very accurate representation of the cognitive perspective, and goes one step further by differentiating between two key dimensions of ISA, namely general information security awareness (GISA) and information security policy awareness (ISPA). GISA thereby corresponds to an individual's overall knowledge and understanding of ISS issues and their potential consequences, while ISPA refers to the knowledge and understanding of the requirements of the organization's ISPs. They argue that those two dimensions are essential for defining ISA because, "… one may be generally aware that using passwords is a necessary precaution but may not know that the organization requires that passwords be changed periodically or that they need to be of a certain length and character composition" (Bulgurcu et al. 2010, p. 533). Thus, one might have a distinct level of GISA but still lack the specific knowledge and understanding of the rules and policies prescribed by their organization. D'Arcy and Hovav (2007a, 2007b, 2008) and D'Arcy et al. (2009) also follow the cognitive stream. Nevertheless, their definition considers IS-users' awareness of an organization's security countermeasures including ISPs, SETA programs, and monitoring activities, rather than their knowledge and understanding of ISS issues and threats as outlined by other scholars of this perspective. Banerjee and Pandey (2010) and Banerjee et al. (2013) reduce their perception of ISA to the knowledge dimension of ISS and define it, "...as the knowledge that members of an organization possess regarding protection of the physical and information assets of that organization." Spears and Barki (2010) also follow the cognitive stream but allude

within their definition to the fact that awareness refers to different target groups of an organization, such as end-users, IS professionals, senior management, and third parties.

3.1.2 Behavioral Perspective

Several definitions do not explain ISA solely as “a state of mind” but also include aspects of actual ISS behavior, which I refer to by the term “behavioral”. These actions range from “acting or responding accordingly to an organization’s ISS rules” (NIST 2003, ISF 2007, Rotvold and Braathen 2008), to “being committed to their security mission” (Siponen 2000, Mancha and Dietrich 2007, NG and Kankanhalli 2008, Rezgui and Marks 2008), to the clear statement that “ISA is one of the information security behaviors“ (Galvez and Guzman 2009). These definitions show that awareness and behavior are closely related to each other, and sometimes the lines between them can be blurry. However, there exists no definition which is solely based on the behavioral perspective.

3.1.3 Process Perspective

The third perspective “process” is based on the perception that ISA is not only a product in the form of a cognitive state of mind or ISS aware behavior, but is described as the actual process to raise awareness. This perspective regards ISA as organizational awareness raising activities and the process of managing these activities (Tsohou et al. 2008). NIST’s (2003) definition of ISA is largely based on the process perspective, since they state that awareness strives to focus on IS-users’ attention on security. Nevertheless, it also incorporates the aspired output (cognitive and behavioral), which is that individuals recognize IT security concerns and respond accordingly (ENISA 2006, Chen et al. 2006, Okenyi and Owens 2007). Kritzinger and Smith (2008) state that ISA “is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with." Others define ISA “as an effort to raise the security consciousness of employees” (Bray 2002), “teach employees to be conscious about information security policies and procedures” (Lim et al. 2006), and as a tool “to stimulate, motivate, and remind the audience what is expected of them" (Peltier 2005). Spurling (1995) argue that ISA campaigns are part of the whole security management process. Similarly, Tsohou et al. (2009) state that ISA „is

an interfunctional process (check, act, plan, do) that crosses different divisional units or departments of organizations".

3.2 Information Security Awareness' Influence on Behavior

There is consensus in the literature that ISA is one of the most essential antecedents of ISS behavior (Dinev and Hu 2007, Bulgurcu et al. 2010, Al-Omari et al. 2012). Nevertheless, it is also argued that ISA alone is not sufficient to explain ISP compliance and ISS behavior (Siponen 2000, Siponen et al. 2009, Anderson and Agarwall 2010). Investigating the processes that underlie the transformation of ISA into behavior has therefore gained increased attention by the community. In the following, a brief introduction to general theory-based behavioral ISS research is given first and subsequently the studies that have investigated the relationship between ISA and behavior empirically are reviewed.

3.2.1 Behavioral Research in the Information Security Domain

The ultimate goal of behavioral research in the context of ISS is to explain why some individuals comply with ISPs while others do not. Aiming to answer this question, a robust body of research has evolved which has investigated a vast number of factors and theories explaining ISS behavior (Puhakainen 2006, Abraham et al. 2011, Lebek et al. 2013a, 2014). According to Lebek et al. (2013a, 2014), 57 different theories have been applied in 113 articles to explain ISS behavior, of which four theories are deemed to be most important and most frequently applied (see Table 9). In the following the four theories are briefly introduced to get a better understanding of the subsequent review of studies that contain the relationship between ISA and behavior (Chapter 3.2.2), since many of them are also based on these theories.

Theory	**#**
Theory of Planned Behavior (TPB)	27
General Deterrence Theory (GDT)	17
Protection Motivation Theory (PMT)	10
Technology Acceptance Model (TAM)	7

Table 9: Most Frequently Used Theories to Explain ISS Behavior (Lebek et al. 2013a)

Theory of Planned Behavior (TPB)

The TPB (Ajzen 1985, Ajzen 1991) is an expectancy-value model that has become one of the most relevant and frequently cited frameworks for predicting intentional behaviors in a great variety of research areas. The theory is based on the assumption that actual behavior is essentially rational and that it results from an individual's intention to perform the corresponding behavior. Although intention does not replace actual behavior, as a strong motivational determinant it accounts for a respectable amount of variance in the actual behavior (Ajzen 1991). According to the TPB, an intention originates from the three belief-based variables of attitude towards the behavior, subjective norm and perceived behavioral control. Thereby attitude is formed by beliefs concerning the consequences of behavior, subjective norm is influenced by normative beliefs (by others) and perceived behavioral control refers to control beliefs and the perception of the ease or difficulty of performing the behavior (Ajzen, 1991). In the practice of ISS, this means that normative beliefs may arise due to an organizational ISS norm, culture, or role responsibility, such as prescribed rules and security guidelines. For fostering an individual's attitude towards ISS, the consequences of following the security guidelines should be desirable. Last, but not least, to increase the perceived behavioral control, the skills and ability to perform ISS compliant behavior should be trained and educated (Siponen 2000).

General Deterrence Theory (GDT)

The GDT (Gibbs 1975) originates from criminology research, and has been adopted to predict various criminal and deviant behaviors by applying the principles of deterrence and sanction fear. GDT suggests that the greater an individual perceives the certainty and severity of potential sanctions for an illicit behavior the lesser the probability that she/he actual commits the corresponding act. In the context of ISS, the GDT is often applied to explain IS misuse and ISP violations (D'Arcy et al. 2009).

Protection Motivation Theory (PMT)

The PMT (Rogers 1975, 1983) is a well validated and robust theoretical framework used to understand why individuals perform recommended behaviors to avert the

consequences of certain threats (e.g., the use of condoms to prevent the spread of HIV, or not smoking to avoid lung cancer). PMT argues that protection motivation – i.e. intention to perform a recommended behavior – is formed by two cognitive appraisal processes that result from different fear appeals: threat appraisal and coping response appraisal. Threat appraisal is based on an individual's fear concerning the perceived severity of the threat (degree of harm associated with the threat), and the perceived vulnerability to the threat. Coping appraisal relies on the belief that the recommended behavior will be effective in reducing the threat (response efficacy) and the belief that one is capable of performing the recommended behavior (self-efficacy). Applying these principles, the PMT is frequently used in ISS research to explain employees' motivation to comply with ISPs and to make use of ISS countermeasures.

Technology Acceptance Model (TAM)

The TAM (Davis 1989) is a well known behavioral theory which suggests that an individual's intention to accept innovative technologies mainly depends on her/his attitude towards use, which in turn is formed by two variables, perceived usefulness and perceived ease of use of the technology. Perceived usefulness is the "the degree to which a person believes that using a particular system would enhance his or her job performance", whereas perceived ease of use reflects "the degree to which a person believes that using a particular system would be free from effort" (Davis 1989). Transformed into the field of ISS, TAM is often used to explain the acceptance of information security technologies or countermeasures, such as ISPs. Perceived usefulness then requires that an employee perceives the consequences of complying with information security guidelines as desirable and effective (Siponen 2000). Ease of use, on the other hand, represents the subjective perceived difficulty or facility of compliance, and is deemed to be quite analogous to TPB's perceived behavioral control. Therefore it can be tackled well by training and education (Siponen 2000).

3.2.2 Studies Investigating the Relationship Between ISA and Behavior

This literature review aims to identify those articles that consider ISA's influence on behavior. Thus, this study clearly differentiates between cognitive ISA and ISS behavior – a distinction which has been neglected by prior analyses. By screening the literature,

21 studies were identified which comply with this criterion. Some studies deviate and test theory-based causal models, others solely show that ISA and behavior are positively correlated to each other. The analysis focused on empirical and conceptual work, since research based on empirical evidence is considered to provide more credible results (Lebek et al. 2013a, 2014), and it is not worthwhile and practicable to include every article mentioning the importance of ISA for ISS behavior. Table 10 gives an overview of the key findings, along with the applied methodology, applied theories, and the type of behavioral outcome. Findings will be critically discussed in section 4.2, below.

The Relationship Between ISA and ISS Behavior (1 of 3)

Author	Applied Theory	Emp. Evid.	Method-ology	Key Findings	Behavior Type
Al-Omari et al (2011, 2012)	TAM	N	Proposed Model	Adapt the technology acceptance model (TAM) by (Davis et al., 1989) and proposes an security acceptance model (SAM) to examine users' behavioral intention to comply with ISPs. The impact of ISA on behavioral intentions to comply is suggested to be indirect via an increase of the adapted TAM's constructs perceived usefulness of IS protection and perceived ease of use of IS protection.	Intention to comply with ISPs
Bulgurcu et al. (2009)	TPB	Y	Quantitative field study: data collected via survey	Draw on the theory of planned beahvior (TPB) by Fishbein and Ajzen (1975) and Ajzen (1991) and shows that ISA and perceived fairness of the requirements of the ISP positively affect attitude, and in turn attitude positively affects intention to comply.	Intention to comply with ISPs
Bulgurcu et al. (2010)	TPB	Y	Quantitative field study: data collected via survey	Found the TPB's constructs attitude towards ISP compliance, self-efficacy and normative beliefs to positively affect an employees' intention to comply with ISPs. Furthermore they show that outcome beliefs about the overall assessment of consequences of compliance and non-compliance (e.g., benefits of compliance, and costs associated with both compliance and non-compliance) significantly influence employees' attitude. ISA in turn was found to increase intentions directly and indirectly through both attitude and outcome beliefs.	Intention to comply with ISPs
Choi et al (2006, 2008)	-	Y	Interviews and quantitative field study: secondary data	Findings suggest that higher levels of managers' ISA increase their actions toward information security which in turn lead to a more efficient and effective organizational performance concerning information security.	Mana-gerial actions towards ISS
D'Arcy and Hovav (2007a, 2007b)	GDT	Y	Quantitative field study: data collected via survey	Apply the general deterrence theory (GDT) and found that IS-users' awareness of computer monitoring seems limited to severe forms of IS misuse, whereas the awareness of countermeasures such as security policies, SETA programs and preventive security software are effective against information security misuse behavior.	IS misuse intention
D'Arcy and Hovav (2008)	GDT	Y	Quantitative field study: data collected via survey	Results indicate that high levels of computer self-efficacy and virtual status increase the deterrent effectiveness of SETA programs and computer monitoring leading to less IS misuse intentions.	IS misuse intention

The Relationship Between ISA and ISS Behavior (2 of 3)					
Author	**Applied Theory**	**Emp. Evid.**	**Method-ology**	**Key Findings**	**Behavior Type**
D'Arcy et al. (2009)	GDT	Y	Quantitative field study: data collected via survey	Empirically test a model which is based on the GDT that posits that user awareness of security countermeasures (e.g., SETA programs, computer surveillance, and ISPs) directly influences the employees' perceived certainty and severity of organizational sanctions associated with IS misuse and in turn leads to reduced IS misuse intention.	IS misuse intention
Dinev and Hu (2007)	TPB, TAM	Y	Quantitative field study: data collected via survey	Results indicate that individuals' awareness of the issues and threats from harmful technologies is a strong antecedent of their intention to use of preventive IS security technologies such as anti-spyware technologies.	Intention to use IS security tech-nologies
Dinev et al. (2009)	TPB, TAM	Y	Quantitative field study: data collected via survey	Applied the same model as Dinev and Hu (2007) and investigated the moderating effects of cultural differences between South Korea and the US. They found that users' technology awareness had weaker effects on their attitudes and intention to use anti-spyware in South Korean users than in the US users.	Intention to use IS security tech-nologies
Galvez and Guzman (2009)	Social Cognitive Theory (SCT), Control Theory	N	Proposed Model	Deviate a model that combines social cognitive theory and control theory in order to explain the individual and environmental factors that influence corporate information security behavior. The main research questions are: How do environmental factors and cognitive factors influence ISS behavior. How does ISA affect ISS behavior?	Infor-mation security practice at work
Kruger et al. (2010)	-	Y	-	Empirically observed a significant relationship between higher levels of ISA (assessed by a simple vocabulary test) and information security behavior.	Infor-mation security behavior
Mancha and Dietrich (2007)	-	N	Proposed Model	Suggest a model that explores the relations between environmental factors (e.g., organizational ISA and organizational security subjective norm) and personality factors affecting accepted peer influence as a determinant of the IS user's attitude toward ISS and ISS behavior.	ISS inten-tions
Ryan (2006)	-	Y	Quantitative field study: data collected via survey	Empirically showed that higher measures of user-level ISA positively affect user information security practice at work and at home environments.	Infor-mation security practice at work and home
Siponen (2000)	TPB, TAM, intrinsic moti-vation	N	Conceptual	Suggests the use of the TPB, the theory of intrinsic motivation (self-determination theory (SDT)), and the TAM to ensure that employees follow ISPs and guidelines. He also suggests personality traits such as morals and ethics, emotions, well-being, a feeling of security, rationality, and logic as important factors influencing individual's motivation to comply with ISPs.	ISP com-pliant behavior
Spears and Barki (2010)	The Emer-gent Inter-actions Theory	Y	Qualitative and quantitative field study: data collected via interviews and survey	The findings indicate that IS users' participation in the ISS risk management process and high levels of awareness of the security risks and controls "…contribute to improvements in both control development (i.e., design and implementation) and performance (i.e., reduced deficiencies and greater efficiency)".	Security control per-formance

The Relationship Between ISA and ISS Behavior (3 of 3)					
Author	**Applied Theory**	**Emp. evid.**	**Method-ology**	**Key Findings**	**Behavior Type**
Straub and Welke (1998)	GDT	Y	Qualitative intervention study	Findings of a cross-sample comparison between two Fortune 500 firms with IT services show that both security trainings and the individual level of security awareness of managers are significantly associated to how well managers can cope with systems risk.	Coping with system risks
Takemura (2011)	-	Y	Quantitative field study: data collected via survey	Discusses the relationship between information security awareness and behavior by analyzing data collected from a Web-based survey on information security measures in Japan. They found a significant influence of employees' level of ISA on their ISS behavior.	Prob-lematic ISS behavior
Thomson and von Solms (1998)	-	N	Conceptual	In this conceptual study, the authors state that security awareness positively affects attitude and other factors that interact with attitude such as cognitions, affections, behavior intentions, and actual behavior.	Infor-mation security practice at work
Yayla (2011)	-	N	Proposed Model	Introduces a model that examines how to control insider threats to information security. Among other factors they identified user awareness as important prerequisite to reduce unintentional insider threats to information security.	Insider threats to infor-mation security

Y = empirical evidence; N = no empirical study has been conducted

Table 10: The Relationship Between ISA and ISS Behavior

D'Arcy and Hovav (2007a) applied the GDT and empirically examined how IS-users' level of awareness of organizational information security countermeasures (security policies, SETA programs, and computer monitoring) influence specific misuse behaviors, such as software piracy, modifying, stealing, destroying data, computer sabotage, and password sharing. They found, that "the deterrent effectiveness of computer monitoring, a more "active" security countermeasure, seems limited to severe forms of IS misuse, whereas the security policies and SETA programs, two "passive" security countermeasures, "appear effective against numerous misuse types that vary in severity." (D'Arcy and Hovav 2007a, p. 22). D'Arcy and Hovav (2007b) extended the model of D'Arcy and Hovav (2007a) by the awareness of the countermeasure "preventive security software", and found that it also significantly reduces users' IS misuse intentions. In another study which is also grounded on GDT, D'Arcy and Hovav (2008) found out that the effects from IS-users' awareness about the before mentioned information security countermeasures on IS misuse intentions are moderated by individual characteristics such as computer self-efficacy and perceived virtual status. The results show that the deterrent effectiveness of SETA programs and computer monitoring is less for computer savvy individuals and more for employees that spend

more working days outside the office. The deterrent effectiveness of an organization's ISP, in contrast, was not found to be moderated by computer self-efficacy and virtual status. In a later publication, D'Arcy et al. (2009) show that the deterrent effects of employee's awareness about management's ISS countermeasures (SETA-programs, computer surveillance, and ISPs) is built indirectly by increasing the employees' sanction perceptions, which are represented by their perceived severity of sanctions and perceived certainty that IT misuse behavior will be revealed. Furthermore, they found that moral reasoning moderated the effect of ISA on intentions.

Bulgurcu et al. (2010) applied a combined model of the TPB, rational choice theory (RCT) and the concept of ISA which is formed by general ISA and ISP awareness. Thereby they found the TPB's constructs attitude towards ISP compliance, self-efficacy and normative beliefs to positively affect employees' intention to comply with their employer's ISP. Furthermore they show that outcome beliefs about the overall assessment of consequences of compliance and non-compliance (e.g., benefits of compliance, and costs associated with both compliance and non-compliance) significantly influence employees' attitudes. ISA in turn was found to increase intentions directly and indirectly through both attitude and outcome beliefs. They argue that ISA programs should be designed in a way that employees' outcome beliefs are reinforced. In addition, Bulgurcu et al. (2009) found that ISA and perceived fairness of the requirements of the ISP are important prerequisites of employees' attitude towards ISP compliance. Also Thomson and Solms (1998) who conceptually analyzed how to educate organizational IS-users effectively, so as to improve and change their information security behavior, identified attitude to be a central factor that interacts with other factors such as cognitions, affections, behavior intentions, and actual behavior. They propose that security awareness comprises all those factors and is therefore a central prerequisite of attitude and behavior. Mancha and Dietrich (2007) provide a research model that suggests individual and environmental factors affect attitude and behavior in a process mediated by the IS-users' level of accepted peer influence. Accepted peer influence is the degree to which IS-users accept influence from others within the organization, and form their attitude toward information security with the expectation of receiving extrinsic or intrinsic incentives. They propose that accepted peer influence mediates the effects of organizational ISA – defined "…as the level in which the users in

an organization are aware of the security mission of the organization (Siponen 2000)" – on attitude which directly increases information security behavioral intentions. They further suggest that the effectiveness of ISA on enhancing accepted peer influence is positively moderated by the personality attribute of conscientiousness.

To understand IS-user behavior towards preventive information security technologies, Dinev and Hu (2007) empirically tested a combined model that builds upon the TPB (Fishbein and Ajzen 1975, Ajzen 1991), TAM (Davis et al. 1989) and technology awareness. The model explains a substantial portion of the variance in an individual's intention to use preventive technologies such as anti-spyware software. They could also verify the positive effects of the three TPB's constructs attitude, subjective norm, and perceived behavioral control on IS-users' intention to use preventive technology. Furthermore, they showed that perceived ease of use precede the level of perceived behavior control, and perceived usefulness strongly determines attitude and moderately determines subjective norm. Awareness, which was defined as "…the user's following, being interested in, and knowledgeable about technological issues, problems, and techniques to solve them" (Dinev and Hu 2007, p. 387) was found to be the central and strong determinant of user attitude and the intention to use preventive technology. In a later publication, and building upon the same model, Dinev et al. (2009) investigated the moderating influence of cultural differences between users from South Korea and the United States on the relationships of the model. Applying the cultural theory developed by Hofstede (1993), they found that users' technology awareness had weaker effects on their attitudes and intention to use anti-spyware in South Korean users than in the US users. Also adapting the TAM, Al-Omari et al. (2011) proposed a security acceptance model. Their model empirically shows that employees' level of awareness of general information security issues, as well as their awareness of protection mechanisms, such as ISPs, SETA programs and computer monitoring indirectly increases their intention to comply via an increase in both the adapted TAM construct's perceived usefulness of information security protection, and perceived ease of use of the protection.

Applying the PMT and the theory of planned behavior, Anderson and Agarwal (2010) state that being aware of security threats influences employees' perceptions of the severity and probability of the threat, which are weighed against their beliefs in the efficacy of their actions, and ultimately influence their security behavior. Galvez and

Guzman (2009) deviated a research model in progress that combines social cognitive theory and control theory in order to investigate different individual and environmental factors that explain employees' information security practice at work. The model suggests a positive direct influence of individual factors, such as outcome expectations in information security endeavors, computer self-efficacy in information security, and perceived obligation. It further suggests environmental factors, such as information security encouragement and support by others as positively influencing corporate information security behavior indirectly, via the above listed individual factors. Last, but not least, they identify ISA as one of the shaping factors, and hypothesize "the higher the information security awareness, the higher the information security practice" (Galvez and Guzman 2009, p. 4). Kruger et al. (2010) primarily aimed to test the feasibility of an information security vocabulary test as an assessment tool for ISA levels of specific topics. However, they also found a significant correlation of the respondents ISA levels and their information security behavior. Ryan (2006) empirically showed that higher measures of user-level ISA positively affect user information security practice at work and in home environments. This was done without applying a theoretical framework.

Siponen (2000) identified the lack of awareness among organizational IS-users in regard to security policies and best practices as a major cause for information security misbehavior. In his conceptual paper, he suggests that fellow scholars consider behavioral theories such as intrinsic motivation and self-determination (Deci and Ryan 1985), the TPB, and the TAM to understand the motivational aspects that lay between ISA and ISP compliant behavior. He further highlights the crucial role of personality traits, such as morals and ethics, emotions, well-being, a feeling of security, rationality, and logic as important factors influencing an individual's motivation to act in accordance with organizational security guidelines. In addition, Yayla (2010) proposes a framework that explains how ISS managers should control intentional and unintentional insider threats to information security. They suggest that increasing employees' levels of ISA, intrinsic motivation, providing security trainings, implementing security tools with a high level of usability, and adjusting time pressure and workload on employees, are effective starting points to reduce unintentional insider threats to information security. On the other hand, to control intentional insider threats, ISS managers should apply

deterrent measures, increase employee integration and commitment, and implement technology-based controls.

Straub and Welke (1998) revealed that ISS risks are often not effectively reduced because managers lack an awareness of the existing range of ISS risk controls. Within two comparative qualitative studies of two Fortune 500 IT services firms they suggest the use of a security risk planning model, an adequate SETA program, and the application of a countermeasure matrix analysis to effectively cope with information systems risks. Thereby they have focused specifically on general deterrence theory. Similarly, within their two studies Choi et al. (2006, 2008) focus on managerial ISA (MISA). Their findings suggest that MISA positively affects the managers' actions toward information security (MATIS) and ultimately enhance the information security performance of the organization. More precisely, they found a positive relationship between MISA and changes in the actions and content of information security strategy, such as ISPs and procedures, information security training and education, information access control, information security systems and programs updates, and information security teams. Hence, to improve an organization's information security performance, it is crucial that managers constitute high levels of ISA. Spears and Barki (2010) conducted a multi-method study at the organizational level that investigates the role of awareness of information security risks and user participation in information security risk management. The findings indicate that IS-users' participation in the information security risk management process and high levels of awareness of the security risks and controls contribute to an improvement of the security control performance of the organization through greater alignment between IS security risk management and the business environment, and improved control development. Last but not least, Takemura (2011) examined "…the relationship between information security awareness and behavior by analyzing data collected from a web-based survey on information security measures in Japan." It was found that individuals with a high level of ISA behave significantly less problematically, in terms of organizational information security measures.

In this chapter the key issues of 21 publications out of the 131 selected ISA studies, which have incorporated an investigation of the relationship between ISA and ISS

behavior have been illustrated. A summary and discussion of the findings will be conducted in Chapter 4.2.

3.3 Antecedents of Information Security Awareness

Increasing employees' levels of ISA minimizes the likelihood of committing information security misbehavior, and enhances the efficiency of protective security techniques and countermeasures of an organization (Galvez and Guzman 2008). Identifying and understanding the factors that influence individuals' awareness of information security is therefore a crucial step to make better use of awareness itself, in order to influence employee ISS behavior and to develop more effective awareness programs. Accordingly, the aim of this section is to identify publications which suggest or investigate antecedents of ISA.

First, the selected publications were screened for studies that empirically examined factors that influence individuals' levels of ISA. Research based on empirical evidence is considered to provide more credible results in terms of its practical usefulness and efficiency than approaches lacking such evidence (Lebek et al. 2013a, 2014). During the review process of the 131 articles, it was recognized that such studies are very limited, not only in terms of numbers but also in term of diversity. The selection was therefore extended to articles which suggest antecedents without the premise that they provide empirical evidence for it. The following analysis follows the cognitive perspective of ISA (see section 3.1.2) and clearly distinguishes between ISA and information security behavior. The identified antecedents of ISA are organized within three dimensions according to their level of origin, namely "individual", "institutional", and "socio-environmental".

3.3.1 Institutional Antecedents

Antecedents of ISA at the institutional level are factors that originate from within the organizational setting and largely rely on an organization's security management practices. The following Table 11 gives an overview of the identified institutional antecedents of ISA, and shows whether or not there exists empirical evidence for the relationship.

Antecedent	Author	Emp. Evid.
Managerial ISA (MISA)	Choi et al (2006)	N
	Rotvold (2008)	N
	Kankanhalli et al. (2003)	N
Management support and commitment	Okenyi and Owens (2007)	N
	Rezgui and Marks (2008)	N
	Tsohou et al. (2010)	N
	Casmir and Yngstrom (2005)	N
	Tu and Yuan (2014)	N
	Rotvold (2008)	N
Security, education, training, and awareness (SETA) program (generic measure)	Wipawayangkool (2009b)	N
	Mani et al. (2014)	Y
Specific SETA method (e-Learning)	Charoen et al. (2007)	Y
	Chen et al. (2006)	Y
	Hagen and Albrechtsen (2009)	Y
Specific SETA method (online game-based training)	Cone et al. (2007)	Y
	Greitzner et al. (2007)	Y
	Fung et al. (2008)	Y
Specific SETA method (password security)	Eminağaoğlu et al. (2009)	Y
Specific SETA method (conceptual change pedagogy)	Chan and Wei (2009)	Y
Specific SETA method (discussion, checklist, web tutorial)	Cox et al. (2001)	Y
Specific SETA method (phishingmail exercise)	Dodge et al. (2007)	Y
Specific SETA method (media richness)	Shaw et al. (2009)	Y
User participation	Rotvold and Braathen (2008)	N
	Albrechtsen (2007)	Y
	Albrechtsen and Hovden (2010)	Y
	Spears and Barki (2010)	Y
	Boujettif and Wang (2010)	Y
	Sommers and Robinson (2004)	Y
Information security policy provision (ISPP)	Albrechtsen (2007)	N
	D'Arcy and Hovav (2007b)	N

Y = empirical evidence; N = no empirical study has been conducted

Table 11: Institutional Antecedents of ISA

Managerial Information's Security Awareness (MISA)

It is a recurrent theme in ISS literature that before employees can build high levels of ISA it is essential for management itself to build a sensibility for the risks and threats of information security. For example, it was found that if top management is aware of the importance of information security, they are more likely to formulate effective ISPs (Kankanhalli et al. 2003). Choi et al. (2008) empirically investigated the effects of

managerial awareness of information security and found that higher levels of MISA lead to more managerial actions towards information security. This is ultimately suggested to increase the efficiency of an organization's information security performance and to enhance employees' levels of ISA (Choi et al. 2008). Rotvold (2008) found that management awareness was one of the few more common reasons given for not conducting security awareness trainings. However, no studies were found that provide empirical evidence for the effects of MISA on employees' ISA.

Management Support and Commitment

Two constructs, which are closely related to MISA and also suggested to have a positive influence on the ISA of employees, are management support and commitment to ISS. Greater management support means that more resources for information security management are available and allocated (Herath and Rao 2009b). Concerning Tu and Yuan (2014), top management commitment toward information security leads to more security practices, such as providing training and awareness programs, which in turn increase ISA. Rezgui and Marks (2008) underline the commitment of management as an important factor impacting users' ISA. Management support was found to be positively related to severe preventive efforts, and to increase the effectiveness of organizational information security (Kankanhalli et al. 2003). Tsohou et al. (2010) emphasize that reasonable resources for security management are essential for establishing sufficient levels of security awareness among employees. Others state that, "… support of senior management is required for any successful awareness program." (Okenyi and Owens 2007, p. 307). Similarly, Casmir and Yanstrom (2005) argue that raising ISA requires good planning and commitment from management. According to Rotvold (2008), management support and commitment is a major cause for the existence or lack of SETA programs within the organization, and that "involving top management and getting their support is essential in building a strong security awareness program" (Rotvold 2008, p. 38). Rotvold further states that high levels of management commitment to information security usually result in creating and improving a better corporate security culture. Tu and Yuan (2014) derive a theoretical model, which investigates the main factors contributing to successful information security management. Besides the hypothesis that management support enhances the security performance of the organization, they

also hypothesize that top management support increases the organization's awareness of security risks and policies. An organization's awareness is thereby represented by the degree to which all employees in the organization are aware of possible security threats, as well as security basics. This research in progress model has not been tested empirically yet. Despite the existence of numerous studies suggesting management support and commitment to be critical antecedents of ISA, it is remarkable that not a single study exists which examines this relationship empirically. The first attempt to do so has been provided by Tu and Yuan (2014). However, their suggested model has not yet been validated. On the contrary, there exists empirical evidence on the effects of management support on behavior (e.g. Herath and Rao 2009b) and on other dependent variables such as the effectiveness of information security management (Kankanhalli et al. 2003), but those studies neglect the effects on ISA as a cognitive state of mind.

Security Education Training and Awareness (SETA) Programs

The term "SETA programs" is frequently used to sum up the great variety of different designs, methods, and nomenclatures of institutional security education, training and awareness raising activities that exist – one of the most essential institutional countermeasures to minimize human-related information security faults and misbehavior (Straub and Welke, 1998, Lee and Lee 2002, Peltier 2005, D'Arcy et al. 2009, Siponen et al. 2009). Employees cannot be blamed for security threats and problems if they are not enlightened as to what such security problems are, and how they can prevent them (von Solms and von Solms 2004, Tu and Yuan 2014). SETA programs aim to actively facilitate the level of organizational ISS by gaining employees' knowledge and awareness of potential security risks, policies, and security responsibilities, and developing the general understanding and skills necessary to perform any required security procedures (Straub and Welke 1998, Aytes and Connolly 2003, Heikka 2008, D'Arcy et al. 2009). The Gartner group states that nothing in the security arena yields as much return on investment (ROI) as security training and awareness programs (Schultz 2004, Wipawayangkool 2009b). Similarly, the international standard of information security ISO/IEC 27002 (2005, p. 26) strongly suggests that, "…all employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in

organizational policies and procedures, as relevant for their job function“. Among the most often used forms of SETA programs are, for example, ISS workshops and seminars (Thomson and von Solms 1998), providing online- and computer-based learning tutorials (Chen et al. 2006), periodic security refresher courses (Hansche 2001a, von Solms and von Solms 2004), periodic newsletters, emails and presentations concerning IS security relevant issues (Spurling 1995, Herath and Rao 2009a), and cues such as posters, flyers, and other awareness material (Crossler and Bélanger 2006).

83 out of the 131 selected publications cover examinations of any kind of SETA programs. Those studies are of a broad diversity examining a vast number of different SETA approaches, methods, contents, or success factors. However, this section focuses on empirical studies that investigate the effects of SETA programs on employees' ISA. Considering every publication solely arguing or mentioning that SETA programs increase ISA would not be practicable, and would not provide significant added value. Furthermore, it is the objective of this chapter to identify antecedents of ISA, rather than to analyze the different SETA program approaches in detail, which is represented by criterion 4 of the classification scheme and out of scope of this paper, as explained in Chapter 2.3. Since the literature around the topic of ISA was first screened comprehensively, six broad streams of SETA research could be recognized. These will be summed up briefly below, with citations from the most important of them. A detailed overview of all six sub-categories of SETA research can be found in Appendix 2-7.

The first stream of SETA studies (n=4) covers comprehensive guidelines for successful SETA program management from an academic point of view (Appendix 2) (e.g. Kritzinger and Smith 2008, Casmir 2005, Banerjee et al. 2013). Comprehensive means that they cover all aspects of the whole management process of SETA programs, which is most often divided into four phases (e.g., need assessment, planning contents and communication methods, implementing the program, and monitoring the effectiveness). Academic means that those studies are published in peer reviewed academic journals. The second stream (n=4) consists of comprehensive guidelines for SETA program management provided by industry standards of good practice (Appendix 3) (e.g. ISO/IEC 27002 (2005, 2013), ENISA 2006, ISF 2007, NIST 2003 and 2006). These studies provide guidance for security managers from a very practical point of view, and highlight the importance of developing effective SETA programs to achieve a satisfying

information security performance within organizations. The third stream (n=11) represents studies providing theoretical frameworks for designing effective SETA programs (Appendix 4) (e.g., Thomson and von Solms 1998, Straub and Welke 1998, Siponen 2000, Puhakainen 2006, Karjalainen and Siponen 2011). These studies are predominantly of a conceptual nature, and the basis of several recommendations for theory and practice. The fourth stream (n=14) covers studies that suggest and validate causal models which incorporate any type of generic SETA construct, examining whether or not the existence of SETA programs in general has significant effects on ISA or ISS behavior (Appendix 5) (e.g. Stanton et al. 2005, D'Arcy and Hovav 2007a, 2007b, D'Arcy et al. 2009, Herath and Rao 2009a). The fifth stream (n=22) is dedicated to examining the effectiveness of specific SETA methods empirically (Appendix 6) (e.g. Cox et al. 2001, Sommers and Robinson 2004, Rahim et al. 2008, NG and Kankanhalli 2008). Studies from this category look at how specific SETA methods, such as "online learning", "security games", "experts presentations", or "training courses" are eligible to increase an employee's ISA and behavior. Last, but not least, the sixth stream (n=30) covers all other practical or academic non-empirical articles, which generally give advice and discuss contents, methods, and success factors for designing effective SETA programs, but do not fit into the first two categories of comprehensive, practical or academic SETA management guidelines, since they do not cover the comprehensive process of SETA management (Appendix 7) (e.g. von Solms and von Solms 2004, Peltier 2005, Steven and van Wyk 2006, Vaast 2007).

To begin with the analysis of studies empirically examining whether or not SETA programs are effective ISS management tools to increase an employee's ISA, the above described sub-categories 4 and 5 of SETA program studies were used. It became evident that the majority of studies consider ISS behavior or intention as dependent variables, but neglect the effects on ISA. Only some studies incorporate a view on ISA as a cognitive state of mind, or even focus specifically on ISA as an output variable. Within cluster four, which summarizes studies analyzing the effectiveness of SETA programs based on generic SETA measures, only 2 out of 13 consider ISA as a dependent variable. Wipawayangkool (2009b) developed a causal model and propose that security trainings in organizations significantly improve the security awareness of employees both at a behavioral and a cognitive level. Furthermore, they suggest that differences in individual

characteristics such as overall job attitude, organizational commitment, and job satisfaction, may moderate the effectiveness of SETA programs for improving ISA. Mani et al. (2014) showed that training employees in current security measures was related to higher levels of ISA. They assign this effect to the mechanism of internalization, which converts explicit knowledge into tacit knowledge. Within cluster five, which covers studies that examine the effectiveness of specific SETA methods, 11 out of 25 show effects on ISA within their observations. 3 out of 11 studies suggest the use of e-learning systems as effective SETA tools to increase employees' ISA. First, Charoen et al. (2007) conducted a case study applying an action research approach, in which they develop and test a training website for creating passwords to fit with theories pertaining to human memory. Participants of their study reported that they gained higher awareness of password security through the training, and obtained better know-how to create secure passwords. "Several users revealed that the e-learning website exposed them to real world threats and provided them with hints and tips to guard themselves against security breaches" (Charoen et al. 2007, p. 66). Second, also conducting a case study, Chen et al. (2006) developed an online-based ISA system which aimed to identify ISA needs and to increase ISA levels amongst the employees of a large insurance company. The findings indicate that an effective e-learning system should provide an information portal, newsgroups, discussion forums, histories of security breach events, security awareness activities, and quality articles to facilitate a frictionless transmission of awareness concepts. Several system users reported that the system helped them to better understand ISS risks, and how they should behave to avoid ISS threats. Last, but not least, Hagen and Albrechtsen (2009) measured and discussed the effectiveness of an e-learning software which trains participants during six modules, covering topics such as general information security, travel security, personal security, security of facilities, and internal/external communication. Their intervention experiment documented significant short-time improvements in ISA and behavior of the 1,208 participants who attended the training. However, a major weakness of the study was the short time frame of the experiment, which did not exceed 3 weeks of intervention.

There exist 3 studies which have tested the effects of game-based training approaches for raising ISA and knowledge of IS-users. All of these studies applied the simulation game "CyberCIEGE", which is described as a highly interactive video game-based

security awareness tool that can support institutional information security training objectives, while engaging the users in an absorbing security adventure (Cone et al. 2007, Greitzner et al. 2007, Fung et al. 2008). Fung et al. (2008) conducted an intervention study in a university environment. Students who played the game for the underlying intervention period appeared to be more able to demonstrate a deep level of understanding in their answers than students from the control group. They ascribe the effect of the game to the fact that the simulation and visualization has given them simulated "real life" experiences. Also, the results of Cone et al. (2007) were positive and show the utility of game-based security trainings in supporting awareness programs. Greitzner et al. (2007) reviewed cognitive principles that can be applied to improve the awareness raising effectiveness in simulation games. Their study revealed that "… effective, serious games must incorporate sound cognitive, learning, and pedagogical principles into their design and structure" (Greitzner et al. 2007, p. 2). The results provide valuable implications that can be used to improve existing game-based awareness training applications in the ISS field.

A number of studies exist which are focused on other diverse specific SETA methods. For example Eminağaoğlu et al. (2009) implemented a password security awareness project over a period of 12 months in a large international transportation enterprise. The project consisted of training and awareness campaigns, and included educational posters, animations and e-messages on the organization's Intranet, as well as surveys and simple online quizzes. 190 randomly selected employees were surveyed by questionnaires and audit meetings at the end of the tenth month of the project. The results showed improved awareness levels of password security issues, as well as an inclined tendency to choose and use their passwords more safely. Chan and Wei (2009) conducted an experiment and found that conceptual change fostered by anomalous data is effective in enhancing information security awareness. Cox et al. (2001) examine a discussion session, a checklist and a web based tutorial as approaches to increasing awareness in an academic setting. They found all three to be successful in raising IS-users' understanding of security, especially because they present the topic in an accessible and interesting way. Dodge et al. (2007) applied a phishing-mail exercise, primarily as an assessment tool for ISA levels of employees. As a side output of the study they found the fishing-mail exercise also to be an effective tool for raising ISA. Finally,

Shaw et al. (2009) have shown that the degree of media richness (e.g., hypermedia, multimedia and hypertext) of SETA programs and the improvement of security awareness levels are positively correlated with each other.

Employee Participation in the Development Process of SETA Programs

In the ISS literature there is a number of studies which show that involving employees in the development process of SETA programs and organizational ISS controls is a valuable method for raising ISA. For example, in an intervention study, which involved employees in different workshops to talk and discuss their opinions on information security to subsequently develop an awareness program, Albrechtsen and Hovden (2010) demonstrated that user participation enhances the participants' ISA and policy compliance behavior. Spears and Barki (2010) empirically tested a model in the context of regulatory ISS compliance in organizations and found that IS-users' participation in the security risk management process increases their awareness of existing security risks and controls significantly. Such participation was also found to contribute to greater alignment between ISS risk-management and business objectives. Rotvold and Braathen (2008) state that information security should not be a passive activity and that it is important that students or employees get involved in the development process of ISS countermeasures. Albrechtsen (2007) interviewed 18 users of an IT-company and a bank about their experience of ISS and their role in reducing ISS violations and threats. The interviewees "…consider a user-involving approach to be much more effective for influencing user awareness and behavior" (Albrechtsen 2007, p. 276). Boujettif and Wang (2010) studied the effectiveness of a highly employee-centered ISA raising methodology that is constructivist in nature, and based on learning autonomy and user integration, rather than on passive and reactive principles. This approach encourages employees to develop their own SETA program materials based on ISA concepts under the guidance of their information security facilitator. Some examples are "email creation and antivirus", "quiz creation", "poster creation", "for and against discussion", "approximations", or "competition". Boujettif and Wang found the constructivist approach to be more effective than classic SETA program approaches, but also point out that one should be aware that this user-centric approach needs more time and resources. Similarly, Sommers and Robinson (2004) tested a SETA approach in which

students develop their own awareness training video and found it to be very effective to foster their ISA levels.

Information Security Policy Provision (ISP Provision)

The constitution of information security policies (ISPs) is a primary resource of institutional ISS management practices (Chan et al. 2005). ISPs represent sets of rules, responsibilities and guidelines which prescribe how organizational ISS resources are used properly and in a secure way (Whitman et al. 2001, Whitman 2008, D'Arcy et al. 2009). Although it has been empirically proven that ISPs are effective to prevent IS-misuse behavior in organizations (Straub and Nance 1990, D'Arcy et al. 2009, Kwon and Johnson 2011), there also exist studies with contradictory results (Wiant 2003, Lee et al. 2004). Accordingly, the literature suggests that the "simple" existence of ISPs is not enough, and highlights the importance of promoting ISPs and ensuring that they are comprehensible, easily accessible and available to employees online, as well as being written in a clear and understandable way. These aspects are summarized in this thesis under the term ISP provision. There exists broad empirical evidence that ISP provision is positively associated with proper ISS behavior (Chan et al. 2005, Herath and Rao 2009b, Siponen et al. 2009, Waly et al. 2012). However, during the review process it was recognized that no study exists which empirically investigates the effects of ISP provision on ISA. However, Albrechtsen (2007) argues that clear and well-defined security policies are an essential part of every awareness program. Furthermore, D'Arcy and Hovav (2007b) state that for enhancing the individual's awareness of security policies, these should be available online and phrased in a manner that is easy to understand. They suggest that an introduction to security policy should take place for all new employees during their first orientation period, and demand that employees sign an acknowledgement of the policies. They further suggest that every employee should be reminded of policies and procedures by displaying them on the internal website at all times.

3.3.2 Individual Antecedents

Antecedents of ISA on the individual level include all factors originating from the employees and IS-users themselves. The following Table 12 gives an overview of the

identified individual antecedents of ISA and shows whether or not there exists any empirical evidence for the relationship.

Antecedent	Author	Emp. Evid.
Information systems knowledge	Ryan (2006, 2007)	Y
Negative experience with ISS threats	Bulgurcu et al. (2010)	N
Individual education	North et al. (2010)	Y
User's security perception	Furnell (2006)	N

Y = empirical evidence; N = no empirical study has been conducted

Table 12: Individual Antecedents of ISA

Information Systems Knowledge (IS Knowledge)

An individual's IS knowledge and similar constructs, such as computer knowledge, personal innovativeness with IT, computer anxiety, computer self-efficacy or technology know-how play a significant role in information security research (Frank et al. 1991, D'Arcy and Hovav 2008, Elie-Dit-Cosaque et al. 2011, Tu and Yuan 2014). During the review process, it was recognized that the relationship between ISA and these constructs has not received intense scrutiny yet. One study was identified that addressed this issue. Ryan (2006, 2007) found out that personal innovativeness with IT and computer self-efficacy had positive correlations with the respondent's levels of ISA, which was defined as employees' understanding of the potential IT security threats and the appropriate countermeasures (Ryan 2007). Computer self-efficacy was defined as individuals' judgment of their capabilities to use computers in diverse situations (Compeau and Higgins 1995) and personal innovativeness with IT was defined as the willingness of an individual to try out new information technologies (Hurt et al. 1977). Although one would expect the constructs around an individual's IS and IT competence to play an important preceding role for ISA, there is a lack of literature investigating these relationships empirically.

Negative Experience with ISS threats

It can be assumed that if individuals have experienced negative ISS incidents and threats in the past, they will gain a sharpened awareness of the risks concerning information security since they have been personally affected by it. However, in the ISA literature,

only Bulgurcu et al. (2010) argue that an individual's awareness of information security may stem from life experiences, such as having experienced a virus attack. Among the identified ISA studies, no one examined this relationship empirically.

Individual Education

North et al. (2010) found that students of technical universities tend to be more aware of information security issues than students of universities with an arts focus. This indicates that the subject of education may affect ISA.

User's Security Perception

In a study of security awareness in both home and organizational settings, Furnell (2006) argues that individuals' perceptions of information security have a significant influence on their awareness of security risks and issues. According to Furnell, security perceptions cover the users' sense of isolation about their system, the reliance upon and great expectations from the Internet service provider and the erroneous perceptions that they are adequately protected.

3.3.3 Socio-Environmental Antecedents

The third category of antecedents that are identified incorporates those factors which are not directly influenced by an organization's management, nor by individuals themselves. Every human behavior is embedded in a situational context and is thus susceptible to interactions with one's environment (Fishbein and Ajzen 1975, Fulk et al. 1987). The issue of environment has not been frequently addressed in the field of ISA research. The suggested socio-environmental antecedents of ISA are summarized in the following Table 13.

Antecedent	Author	Emp Evid.
Secondary source's influence (massmedia, news, security journals)	Bulgurcu et al. (2010)	N
	Al-omari et al. (2011)	N
	Dinev et al (2009)	N
	Mani et al. (2014)	Y
Public Awareness	Siponen (2000, 2001)	N
	Rezgui and Marks 2008	N
Peer Behavior	Furnell (2006)	N
	Leach (2003)	N
	Mani et al. (2014)	Y
	Dinev et al. (2009)	N

Y = empirical evidence; N = no empirical study has been conducted

Table 13: Socio-Environmental Antecedents of ISA

Secondary Source Influence

Several studies in the ISS domain show that individuals' information security behavior is impacted by information received from secondary sources such as newspapers, radio, the Internet, and TV (NG and Rahim 2005, Siponen et al. 2009). Similarly, Bulgurcu et al. (2010) and Al-omari (2011) both argue that an individual's ISA is built from life experiences and from external resources, such as the Internet, newspapers, or security journals. Furnell (2006) emphasizes that information about ISS in the media may have a positive impact on the public awareness towards information security matters. Dinev et al. (2009) suspect that media influences on users' awareness may be much less in areas where opinions of social groups and leaders are highly valued, such as Korea (Dinev et al. 2009). In contrast, they suspect a much greater influence of the media on US users. Last, but not least, Mani et al. (2014) found that individuals can develop explicit ISS knowledge by combining information received from formal documents or the mass media.

Public Awareness

Another social-environmental factor is the public awareness of information security (Siponen 2000, 2001). The way the public views security issues and threat will affect the individual's perception of information security (Rezgui and Marks 2008).

Peer Behavior

Empirical evidence shows the positive impact of ISP compliant behavior of peers on the information security behavior of others (Aytes and Connolly 2003, Chan et al. 2005, NG and Rahim 2005, Herath and Rao 2009a, Siponen and Vance 2010). The motivating effects of peer behavior can largely be ascribed to a human's desire for approval from significant others (Ajzen's, 1985), but also because interactions with peers enables knowledge transfer (Spears 2006). Leach (2003) argues that the knowledge transfer resulting from observing the security behavior of co-workers has an impact on employees' ISA. Furthermore, Dinev et al. (2009) and Furnell (2006) suggest that the values of the social group that the individual interacts with impacts the user's view on awareness. Mani et al. (2014) found that business employees gained ISA through conversations with friends and through learning from other people's computer incident stories. They name this effect socialization. However, existing studies examining the effects of peer behavior on ISA are very generic and largely lack empirical evidence.

4 Discussion

This study reviews the current state of the literature on ISA research by applying an open coding technique based on grounded theory (Strauss and Corbin 1990). The in-depth analysis of the literature was guided by three pre-defined research questions on the topic. First, it was of interest how the literature conceptualizes and defines ISA. Subsequently, it was analyzed how existing studies explain the process underlying the transformation of ISA into ISS behavior. Finally the review examined factors that are suggested to influence individuals' ISA. 131 publications that deal with ISA were identified through screening a broad variety of information systems journals, specific ISS journals, conference proceedings, and doctoral dissertations. In the forthcoming sections the findings are critically analyzed and discussed, theoretical and practical implications are given, and gaps for future research are pointed out. Finally, the study's limitations as well as a conclusion are set down. The structure of the discussion is organized according to the three research questions RQ1, RQ2, and RQ3 which are outlined in Chapter 1.

4.1 Definitions of Information Security Awareness

The first aim of this study was to analyze how the literature perceives and conceptualizes the domain of ISA. Within 131 publications dealing with ISA, 21 different definitions were found. A further 17 studies were identified which explicitly followed one of the 21 definitions. By looking at the different definitions, it becomes clear that even though substantial research on the subject has been conducted, the literature lacks a coherent conceptualization of ISA. Moreover, the majority of studies do not even define the topic at all. The analysis of the definitions revealed that literature's perception of ISA can be categorized into three main categories, namely "cognitive", "behavioral", and "procedural". From the cognitive perspective, ISA represents an individual's state of mind, which is characterized by recognizing and understanding the importance and significance of ISS and being aware and conscious about ISS objectives, risks and threats, and having the required knowledge to use IS responsibly. Behavioral aspects of ISA cover IS-users' actual ISS behavior and ISP compliance, such as acting or responding accordingly to an organization's ISS rules. The third perspective

"procedural" perceives ISA as organizational awareness raising activities (SETA programs) and the process of managing these activities. Hence, ISA is perceived as a multidimensional issue that covers one, two, or even all of the three aspects. This conclusion comes close to the results of Tsohou et al. (2008), although they distinguish solely between process and product aspects. Accordingly, there exist different understandings of what ISA can actually mean, and therefore also different angles from which it can be approached and analyzed.

It is a recurrent theme in ISS literature that individuals' cognitive awareness of ISS issues is necessary to enable ISS behavior, and that ISA alone is often argued to be insufficient (Siponen 2000, Siponen et al. 2009, Anderson and Agarwall 2010). Accordingly, one can gain a high level of ISA through awareness programs but still not comply with the organization's ISP. In conclusion, ISA raising processes represent an input variable of ISA, whereas behavior represents an output variable. This important differentiation is neglected by those studies which comprehend ISA as ISS behavior or even as the process of raising ISA itself. Although it is obvious that ISA raising activities, awareness as cognitive state of mind, and ISS behavior are closely correlated with each other, there is a need in the literature to clearly distinguish these terms from each other, and to achieve an universal and congruent understanding of what ISA represents. Studies are needed which address this issue in more depth by analyzing the nature of ISA, and develop a framework which can serve as a base for a coherent and clear assignment of the topic. A first attempt in doing so was accomplished by Wipawayangkool (2009a) who applied the theory of learning outcomes by Kraiger et al. (1993) and developed a conceptual framework that describes an awareness state and a behavior state of ISA. Furthermore the concept graduates the awareness state into a cognitive dimension (tech and non-tech knowledge) and an affective dimension (attitude and motivation). Based on the principles of scientific realism, they suggest that researchers need to apply multiple methodologies in order to study security awareness in a more effective manner and to capture and learn better the multidimensional nature of ISA. Another interesting approach is outlined by Helisch and Pokoyski (2009) [1] who

[1] Books were not included within the selection of analyzed publications

state that ISA is an interplay of knowledge, capability, and desire as illustrated in Figure 11.

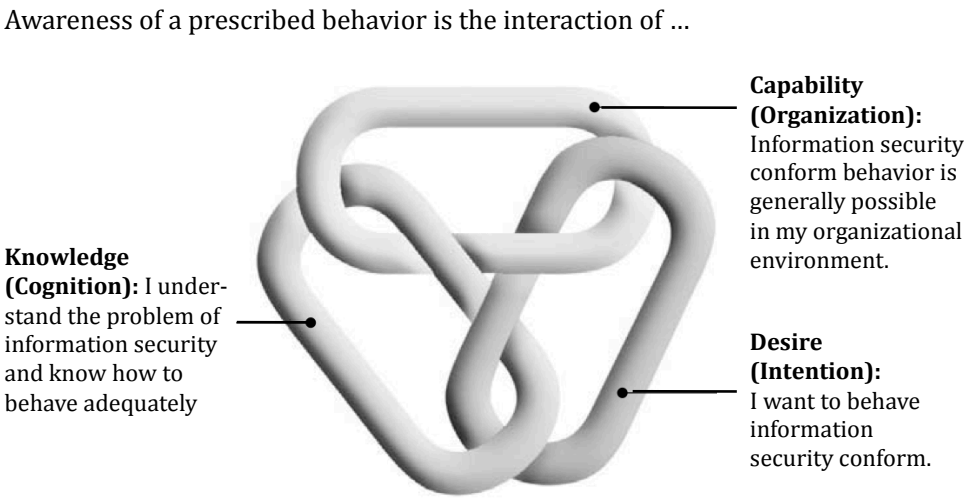


Figure 11: Information Security Awareness (Helisch and Pokoyski (2009)

Future research should consider the findings and insights provided by this review as starting point to delve deeper into conceptualization and nature of ISA. Thereby, it would be appealing to apply perspectives of other disciplines such as marketing psychology, philosophy, or sociology.

4.2 Information Security Awareness' Influence on Behavior

The next focus of this review was to provide fellow scholars and practitioners with insights into the mechanisms that transform an individual's cognitive ISA into actual ISS behavior. While 115 empirical studies exist applying 57 different multidisciplinary theories to explain why some individuals comply with ISPs while others do not (Lebek et al. 2013a, 2014), it is surprising that only a minority of studies (n = 21) incorporates the relationship between ISA and behavior, despite the fact that the literature regards ISA as one of the central antecedents of behavior (Dinev and Hu 2007, Bulgurcu et al. 2010, Al-Omari et al. 2012). Thus, a short-coming of prior empirical research on ISS behavior is that it neglects the concept of cognitive ISA, or at least does not control for it. Looking at studies incorporating the relationship between ISA and behavior, these can be divided into studies which empirically test suggested theory-based models, and others which solely show a direct significant correlation between ISA and behavior. Within the 21

publications, the most frequently applied theories are the general deterrence theory (GDT), the theory of planned behavior (TPB), and the technology acceptance model (TAM). In conclusion, the analysis of the 21 studies reveals five important mediating constructs through which ISA affects behavior indirectly. These are illustrated in the following three passages.

First, the GDT argues that ISA influences the IS-users' perceived certainty that harmful ISS behavior will be sanctioned as well as the severity of those sanctions, and that this effect indirectly decreases their IS misuse intentions. Hence, deterrence-based studies suggest that managers clearly communicate that harmful ISS behavior and ISP violations will be detected and consequently sanctioned. Most of these studies define ISA as awareness of security countermeasures specifically (e.g., ISPs, SETA programs, computer monitoring), but neglect the general dimension of ISA (GISA), such as described by Bulgurcu et al. (2010). Future deterrence studies should incorporate a measure of GISA. Moreover, it was found that the deterrent effectiveness of active security countermeasures, such as computer monitoring is less effective than passive security countermeasures, such as security policies and SETA programs (D'Arcy and Hovav 2007a). Scholars should delve deeper into the effectiveness of various ISS countermeasures.

Second, studies from the TAM perspective suggest that protecting information security and using preventive information security technologies should be perceived as useful and easy to use (Dinev and Hu 2007, Dinev et al. 2009, Al-Omari et al. 2011). Thus, practitioners should aim to communicate the effectiveness of ISS security countermeasures and to increase their use practicability as far as possible. It would also be interesting to see whether there are differences between different specific preventive ISS technologies.

Third, according to studies based on the TPB, a positive attitude towards policy compliance is an important partial mediator between ISA and policy compliant behavior (e.g., Dinev and Hu 2007, Mancha and Dietrich 2007, Bulgurcu et al. 2009 and 2010). Therefore it is an appealing road for future research to discover how employees' attitudes towards ISP compliance can be influenced positively. The first attempts at doing so are provided by some studies. For example, Dinev and Hu (2007) combined

TPB and TAM and found that perceived usefulness of preventive ISS technologies determines an IS-user's attitude towards ISP compliance. Bulgurcu et al. (2010) showed that employees' outcome beliefs and consequence beliefs of their ISS actions have a positive effect on their attitudes towards ISP compliance. Those outcome beliefs are also known to be higher if ISA is high (Bulgurcu et al. 2010). However, conventionally applied SETA programs usually only aim to gain awareness and knowledge of existing ISS threats and develop skills to apply proper ISS countermeasures, but neglect to improve the recipients' attitude (Aytes and Connolly, 2003, Heikka 2008). Against this background, security managers should design SETA programs not just with the aim of increasing ISA and ISP compliance but also in a way, that reinforces employees' outcome beliefs and attitudes.

Although the literature based on GDT, TPB and TAM provides important insights into the question of how ISA influences behavior, our understanding as to the processes that are liable to affect this relationship is still scarce (Bulgurcu et al. 2010). For example, while we know much about the role of deterrents, our understanding regarding the potential of individuals' motivations to comply beyond coerced enforcement, as suggested by Siponen (2000), remains limited. Although several studies show that deterrence and ISP compliant behavior are positively correlated, some studies did not confirm the positive effects of deterrence (e.g., Pahnila et al. 2007a, D'Arcy and Herath 2011, Hu et al. 2011). Hence, deterrence seems not to be enough to explain ISP compliance. Addressing this issue, Siponen and Vance (2010) showed that invoking neutralization techniques and rationalizing (e.g., refusal of responsibility and guilt, blame from others, or compensation of harmful behavior with creditable behavior), can reduce the effects of deterrence. More studies are needed that explore possible answers to the question of why deterrence seems not to be enough. Future studies should seek to discover employees' ISP adherence behaviors from other motivational perspectives, such as the self-determination theory (SDT) and the protection motivation theory (PMT), and combine them with the concept of ISA. Prior studies based on the PMT (e.g. Siponen et al. 2006, Herath and Rao 2009b, Johnston and Warkentin 2010) do not incorporate ISA as a preceding variable. Moreover, directly comparing the two competing concepts GDT (based on coerced enforcement) and SDT (based on autonomy) would be an appealing avenue for future research, especially because threats

and fear appeal are known to be counterproductive in some cases (Workman et al. 2009).

There are studies which indicate that the process of transforming ISA into behavior may be moderated by several individual characteristics. For example, D'Arcy and Hovav (2008) found that the effects of ISA on IS misuse intentions are moderated by individual characteristics, such as computer self-efficacy and perceived virtual status. More specifically, the results show that the deterrent effect of SETA programs and computer monitoring is weaker for computer savvy individuals and for employees that spend more working days outside the office. D'Arcy et al. (2009) found that an individual's moral reasoning moderated the effect of ISA on intentions. Mancha and Dietrich (2007) suggested that the effectiveness of ISA in enhancing ISS behavior is positively moderated by the personality attribute conscientiousness. Also, Siponen (2000) has argued that personality traits such as morals and ethics, emotions, well-being, a feeling of security, rationality, and logic should play a crucial role in the relationship between ISA and behavior. There is a paucity of studies addressing the effects of individual characteristics on the relationship between ISA and behavior empirically. This gap should be closed by future research.

The majority of studies have focused on IS end-users' ISA. However, some studies are dedicated to investigating the subject from a management perspective. These studies indicate that managers with high ISA levels take significantly more and better actions to protect the organizational information assets (Straub and Welke 1998, Choi et al. 2006 and 2008). Although Spears and Barki (2010) do not specifically investigate managerial ISA, they show that high levels of ISA amongst individuals involved in the ISS risk management process lead to enhanced ISS performances, through greater alignment between ISS risk management and the business environment. Due to the strong practical relevance, investigating the effects of MISA on managers' actions and organizations' security performances should gain more attention in the community.

Studies of criterion 2 also have several limitations. First, most of the findings relied heavily on users' perceptions, to explain security behavior, which might not necessarily reflect actual behavior (Straub et al. 1995, Kruger and Kearney 2006, Anderson and Agarwal, 2010). Future studies should aim to observe actual behavior, although this is

known to be very difficult in most cases (Vroom and von Solms 2004). This aim could be achieved, however, by analyzing user logs, or applying experimental study designs, for example (Workman et al. 2008). Measuring true behavior as a dependent variable, however, will always remain a major challenge in ISS research methodology (Crossler et al. 2013). Furthermore, prior studies focus on intentional behavior (e.g., ISP compliance intentions or IS misuse intentions). Thus, they don't provide conclusions about individuals who unintentionally violate prescribed ISS procedures and policies. This differentiation is important, since one might have the intent to comply with ISPs but still violate them without even recognizing the fact. Second, the majority of studies used very generic measures of intentional ISS behavior, such as ISP compliance or IS misuse intentions. There is a lack of studies investigating the relationship between ISA and more specific behaviors, such as password management, log in behaviors, proper use of antivirus software, or ISS behavior with regard to mobile devices, such as smart phones and tablets. Third, since changing attitudes is considered to be a long-term task (Siponen 2000), longitudinal study designs are needed to explore how attitudes towards ISP compliance can be changed in the long run. Longitudinal and laboratory studies are rare and need to be fostered and encouraged in order to enrich the field of behavioral research (Crossler et al. 2013). Last, but not least, there is a high concentration of samples collected within Western cultures, meaning that cultural differences are not taken into account. Dinev et al. (2009) found that users' technology awareness had weaker effects on their attitudes and intention to use anti-spyware in South Korean users than in US users. Future research should investigate in more depth the influence of cross-cultural differences on the relationship between ISA and ISS behavior.

4.3 Antecedents of Information Security Awareness

The third goal of this study is to identify publications which suggest or empirically investigate potential antecedents of employees' cognitive ISA. Identifying and understanding the factors that influence ISA is crucial for management to develop more effective awareness programs, and to make the entire process of achieving beneficial security behavior more efficient. Within 131 selected publications, various suggested antecedents of ISA are identified. Based on the open coding analysis, these antecedents

are classified into institutional, individual, and socio-environmental determinants of ISA according to their levels of origin.

While there exists a large body of empirical literature investigating factors that influence information security behavior (Abraham et al. 2011), it is noticeable that, despite the importance of employees' ISA within the ISS domain, there is a remarkable lack of studies investigating antecedents of ISA empirically. This finding confirms the presumption of Bulgurcu et al. (2010, p. 543) that "…identifying the factors that lead to information security awareness would be an important contribution to academics, since there is a gap in the literature in this direction". Future research is needed which tests the hypothesized effects of various suggested individual, institutional and environmental antecedents of ISA empirically.

At the institutional level, managers' awareness of information security as well as their support and commitment are suggested to positively correlate with employees' ISA levels. In conclusion, it is a premise that management itself builds a sensibility for the risks and threats of information security, and that it provides sufficient support to its organization's IS-users. By far the most essential instruments for supporting employees, raising awareness and ultimately fostering policy compliant behavior are security education training and awareness (SETA) programs. SETA programs are one of the few antecedents for which empirical evidence exists. These studies prove the effectiveness of generic SETA programs and various specific SETA methods (e.g., video games, discussion sessions, web-tutorials) (see Table 11 in Chapter 3.3). How these programs should be designed to be most effective is a large field of research. This is not an objective of this study. However, an overview on this topic is shown in Appendix 2 – 7. Nevertheless, most studies in this field focus on the effects of SETA programs on behavior, but do not investigate their usefulness to raise ISA. Since it is argued that most misbehaviors result from a lack of awareness, more intervention studies should explore which methods are most effective to raise ISA. Thereby it would be interesting to explore if the effectiveness of SETA programs varies depending on different individual factors such as overall job attitude and organizational commitment (Wipawayangkool 2009b). It has been found that integrating IS-users into the actual process of developing SETA programs is a very effective way to increase their ISA levels. Managers should keep this in mind and integrate their employees into the process of developing SETA

programs. Last but not least, the literature argues that the provision of ISPs, in the sense that they are understandable for all employees and easily accessible on- and offline at any time, would enhance employees' awareness of the rules and responsibilities regarding information security issues. This is a very economic and easy way to increase employees' ISA. Future studies should seek to verify this assumption empirically.

On the individual level, general knowledge of information systems, the type of education (e.g. technical vs. non-technical), as well as prior negative experience with ISS threats and incidents are argued to be determinants of ISA. To avoid unintentional misbehavior, practitioners should therefore seek to improve the skills of employees who lack general IS knowledge, and further, should clearly communicate the damages the organization had to struggle with after prior policy violations and cyber-attacks. However, since empirical evidence is rare, further research should validate these hypothesized effects.

On the socio-environmental level, information about ISS incidents received from secondary sources, such as newspapers, radio, the Internet and TV, the general public awareness of information security, as well as the observed behavior of peers and colleagues are suggested to be potential prerequisites of ISA. This advises management to spread public information about ISS incidents among the staff of the organization, and to make ideal behavior of peers as transparent as possible. In this regard, it could be beneficial to organize regular discussion rounds, where role model employees can tell other employees how they handle critical ISS issues. Since antecedents of ISA on the socio-environmental level have not received much empirical attention yet, future research is needed to close this gap.

Besides the empirical validation of the above-suggested factors, future research should delve deeper into this important facet of ISA research, aiming to explore further potential antecedents. It can be assumed that many of the factors which are known to affect ISS behavior may also have their impact on awareness, since those variables are very closely related to each other. In this regard, the works of Siponen (2000), Galvez and Guzman (2006), and Abraham et al. (2011), who identified factors that influence corporate information security behavior, can serve as valuable sources. Recently, an increasing volume of research suggests the importance of developing an information security culture within the organization to ensure ISS behavior of employees (Furnell

and Thomson 2009, Talib et al. 2010). Scholars should investigate how establishing an information security culture within an organization is related to the ISA levels and ISP compliant behaviors of its employees. Furthermore, it would be interesting if ISA also played a mediating role between some of the antecedents of behavior and behavior itself, especially those which affect the knowledge dimension of ISS, such as SETA programs, IS knowledge, or ISP provision. Scholars could also investigate if the awareness of different types of stakeholders or hierarchy levels (e.g., management, employee, third party) depends on different influencing factors. For example, it would be appealing to know the factors that specifically build managerial ISA (MISA), since MISA was found to be essential for the overall ISS performance of an organization (Choi et al. 2008). This knowledge can be used to customize security awareness programs more specifically aimed at the target group. Similarly, the effect of cultural differences could receive more attention within the community, since one of the biggest limitations of behavioral ISS research is that the majority of it has been conducted in Western cultures (Crossler et al. 2013). For example, media influence on users' awareness is suspected to be much less in areas where opinions of social groups and leaders are highly valued, such as in Korea (Dinev et al. 2009).

4.4 Summary of Future Research Recommendations

The following Table 14 provides a summarized overview of the future research recommendations identified within this study according to the three analyzed criteria.

Criterion	Summary of Future Research Recommendations (1 of 2)
1	Future research should address the vague and heterogeneous conceptualization of ISA by exploring the nature of ISA in more depth and developing a generally accepted framework, which can then serve as a base for a coherent and clear assignment of the topic.
2	Future empirical studies on ISS behavior are strongly recommended to take more thorough account of the effects of cognitive ISA.
2	Deterrence studies are needed that do not only apply awareness of security countermeasures specifically (e.g., ISPs, SETA programs, computer monitoring), but incorporate a general dimension of ISA (GISA) such as described by Bulgurcu et al. (2010)
2	Delving deeper into the question how employees' attitudes towards information security can be influenced positively. Since changing attitudes is considered to be a long-time task (Siponen 2000a), longitudinal study designs are needed to explore how attitudes towards ISP compliance can be changed on the long run.
2	Studies are needed that explore possible answers to the question why deterrence seems not to be enough. Future research should investigate individuals' compliance motivation from perspectives beyond coerced enforcement, such as self-determination and the consideration of personal values.

Criterion	Future Research Recommendations (2 of 2)
2	Studies should explore the potential moderating effects of individual characteristics and traits on the relationship between ISA and behavior empirically, such as e.g., morals and ethics, emotions, well-being, a feeling of security, rationality, and logic, as proposed by Siponen 2000.
2	Due to the strong practical relevance, investigating the effects of managerial information security awareness (MISA) on manager's actions and organizations' security performances should gain more attention in the community.
2	Future studies should aim to observe actual behavior, although this is known to be very difficult in most cases (Vroom and von Solms 2004). This could be done for example by analyzing user logs or applying experimental study designs (Workman et al. 2008).
2	The majority of studies used very generic measures of intentional ISS behavior such as ISP compliance or IS misuse intentions. Future studies should apply more specific behaviors such as e.g. password management, log in behaviors, proper use of antivirus software, or ISS behavior with regard to mobile devices such as smart phones and tablets.
2	The effect of cultural differences should receive more attention within the community since one of the biggest limitations of behavioral ISS research is that the majority of it has been conducted in Western cultures (Crossler et al. 2013).
3	"…identifying the factors that lead to information security awareness would be an important contribution to academics, since there is a gap in the literature in this direction" (Bulgurcu et al. 2010, p. 543). Future research is needed, which tests the hypothesized effects of various suggested individual, institutional and environmental antecedents of ISA empirically.
3	Most studies that investigate the effects of SETA programs focus on behavior but do not investigate their usefulness to raise ISA. Since it is argued that most misbehaviors result from a lack of awareness, more intervention studies should explore which methods are most effective to raise ISA.
3	Scholars should investigate how establishing an information security culture within an organization is related to the ISA levels and ISP compliant behaviors of its employees.
3	There is a need to explore if ISA plays a mediating role between some of the antecedents of behavior and behavior itself, especially those which affect the knowledge dimension of ISS such as SETA programs, IS knowledge, or ISP provision.
3	Scholars should investigate if the awareness of different types of stakeholders or hierarchy levels (e.g., management, employee, third party) depends on different influencing factors.
3	Differences in individual characteristics such as e.g., workload, overall job attitude, or organizational commitment could have an impact on the effectiveness of ISA raising activities (Wipawayangkool 2009b). Future research is needed to address this issue empirically.
general	Future studies should especially seek to analyze the different assessment approaches for employees' ISA in more depth as represented by criterion 5.
general	The effect of cultural differences should receive more attention within the community since one of the biggest limitations of behavioral ISS research is that the majority of it has been conducted in Western cultures (Crossler et al. 2013).

1 = Definition of ISA; 2 = ISA's Relationship with Behavior; 3 = Antecedents of ISA

Table 14 Summary of Future Research Recommendations

4.5 General Limitations of the Literature Review

As with any other academic study, this literature review of ISA research does not come without limitations. Although the structured approach for gathering literature proposed by Webster and Watson (2002) is applied, there are some limitations regarding the selection of the literature. The review focuses on English publications only and neglects publications in other languages. Furthermore non-peer-reviewed publications, such as books and whitepapers, as well as publications of bad quality were excluded in the review process. Hence, some research contributions might be missing in the analysis. Last but not least, although the review identified the ISA literature as comprehensively as possible, the in-depth analysis focused on criterion 1, 2, and 3 of the classification scheme but excluded the identified criterion 4 and 5. Since there already exist reviews on SETA programs (criterion 4), future studies should especially seek to analyze the different assessment approaches for employees' ISA in more depth, as represented by criterion 5.

4.6 Conclusion

The information security awareness (ISA) of employees is an evolving research field and plays a key role in protecting organizations against cyber attacks and information security incidents. This study provides an extensive review of the current state of the literature on ISA research. By applying an open coding technique based on grounded theory, the literature is first comprehensively screened and categorized into five main subfields, of which three are subjected to an in-depth analysis, namely "definitions of ISA", "ISA's influence on ISS behavior", and "antecedents of ISA". Subsequently, the findings are critically discussed, implications for theory and practice are given, and recommendations for future research directions are pointed out.

D. Study II: Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior[2]

Abstract

Information security awareness (ISA) is referred to as a state of consciousness and knowledge about security issues and is frequently found to be an essential antecedent of behavior. However, to date we know little about the factors influencing ISA and its mediating effect on information security behavior. This study addresses this shortcoming by proposing a research model that investigates ISA's institutional, individual, and environmental antecedents, and examines the mediating role of ISA. The model was empirically tested with survey data from 475 employees. The model explains a substantial proportion of the variance of ISA (.50) and intention to comply with information security policies (.40). The results imply that the provision of security policies, together with employees' knowledge of information systems, are the most influential antecedents of ISA. The study shows that ISA mediates the relationship between ISA's antecedents and behavioral intention. The findings will be useful for stakeholders interested in encouraging employee behavior compliant with information security policy (ISP).

[2] An earlier version of this paper was presented at the International Conference of Information Systems (ICIS 2013) in Milan, Italy, December 15-18, 2013.

1 Introduction

The functioning of most organizations greatly relies on corporate information systems (IS). Thus, managing risk associated with security threats is becoming increasingly important, since violations of information security often have serious financial and reputational consequences for companies and their customers (Cavusoglu et al. 2004). Ensuring information systems security (ISS) has become one of the major priorities and challenges for organizations. Consequently, academia and businesses are interested in how ISS threats can be reduced effectively (D'Arcy et al. 2009). Although organizations spend evermore money on technological solutions to safeguard information security, anecdotal and empirical evidence implies that the number and severity of incidents is growing (The Economist 2014). Similar to this trend in organizations, prior research on ISS was mainly focused on technological issues, such as encryption technology, spyware and virus detection, or firewalls (Spears and Barki 2010).

However, it is assumed that 50 - 70 % of overall ISS incidents in organizations result either directly or indirectly from employees' misuse - ranging from naïve mistakes to intentional harm (Ernst and Young 2003, Siponen and Vance 2010). Therefore, improving information security needs both investments in technical and socio-organizational resources (Bulgurcu et al. 2010). Against this background, recent studies shifted the focus to organizational, environmental, and individual factors that influence employees' behavior, as they are regarded as the weakest link in information security (Siponen 2000, Boss et al. 2009, Bulgurcu et al. 2010). Prior research has found that increasing employees' ISA has a strong positive effect on their ISP compliant behavior (Dinev and Hu 2007, D'Arcy et al. 2009, Bulgurcu et al. 2010). Also, managers claim that establishing a sufficient level of ISA is one of the priorities of security management (Tsohou et al. 2008). In this regard, security management refers to making employees aware of their behavior's potential ramifications for information security, and qualify them to use organizational IS resources responsibly (NIST 2003).

Although ISA's important role is widely recognized, our understanding as to the factors influencing ISA is scarce. Extant ISS studies suggest the existence of different factors preceding ISA. However, there is a lack of studies investigating antecedents of ISA empirically. Accordingly, in a special issue of the MIS Quarterly, Bulgurcu et al. (2010)

state that "… identifying the factors that lead to information security awareness would be an important contribution to academics, since there is a gap in the literature in this direction, as well as to practitioners, since they can use these factors to formulate their information security awareness programs." (p. 543). This study aims to add to the limited research on ISA, and delves deeper into Siponen's (2000) assertion that "ISA is one of the most important antecedents of behavior" by investigating the important, yet underexamined, mediating role of ISA on the relationship between ISA's antecedents and the intention to comply with information security policies (ISPs).

The remainder of the paper is structured in six sections. In the following paragraph, prior research on ISA and ISS behavior is reviewed and some theoretical background is elaborated. In Section 3 the research model is presented and the study's hypotheses are derived. Subsequently, the methodology is outlined (Section 4) and the results are presented (Section 5). The paper concludes with a discussion of the results, and provides the implications for research and practice (Section 6).

2 Background

Owing to the socially constructed nature of ISA, no universal definition exists in the literature. By carefully reviewing the ISS literature, three different perspectives on ISA were identified. These are “procedural”, “behavioral”, and “cognitive”. From a procedural perspective, the methods and different developmental phases of ISA, such as the planning and execution of awareness raising initiatives are at the core (e.g., NIST 2003, Lim et al. 2010, Rastogi and von Solms 2012). The behavioral perspective, meanwhile, puts emphasis on behavioral dimensions affecting ISA, such as the employee's intention to act responsibly or comply with IS policies. These actions range from "being committed to information security" (Siponen 2000, Rezgui and Marks 2008) to "help […] effectively protect the organization's information assets" (Rotvold 2008). Most commonly, however, ISA is studied from a cognitive perspective, as in the present study.

ISA, is then defined as an employee’s state of mind, which is characterized by recognizing the importance of ISS, being aware and conscious about IS security objectives, risks and threats, and having an interest in gaining the required knowledge to use IS responsibly, if it is not already present (Siponen 2000, Straub and Welke 1998, Thomson and von Solms, 1998). Bulgurcu et al. (2010) additionally differentiate between the two ISA dimensions of general information security awareness (GISA) and information security policy awareness (ISPA). GISA corresponds to an individual’s overall knowledge and understanding of ISS issues and their potential consequences, while ISPA refers to the knowledge and understanding of the requirements of the organization’s ISPs. This study follows the definition of Bulgurcu et al (2010) and conceptualizes ISA as a second order construct.

The investigation of ISA and its important role for ISS in organizations is still a young subfield of ISS literature. One main stream of ISA research is dedicated to the question of how ISA can be fostered by the application of security education, training, and awareness (SETA) programs (Puhakainen and Siponen 2010). Accordingly, different designs, methods, and effects of SETA programs have become the subject of this stream (e.g., Thomson and von Solms 1998, Peltier 2005, Puhakainen 2006, Rotvold and Braathen 2008, Puhakainen and Siponen 2010, Karjalainen and Siponen 2011).

Spurling (1995), for example, recommends the building of a company-specific process, which should be in conformity with the corporate culture. He particularly emphasizes the use of presentations, training sessions, emails and newsletters in order to foster information security awareness within organizations. Others make use of design theory to improve awareness-raising programs (Puhakainen 2006). Rotvold (2008) asserts that the goals of awareness programs need to be clearly communicated and repeated often. She also suggests that messages within those programs should regularly be assessed for their effectiveness and, if necessary, be modified to ever changing exigencies of the organization's security environment. Peltier (2005) points out that an awareness program is supposed to deliver the security information in an appealing way, because most employees lack the time and enthusiasm to actually read all the information pamphlets and security policies. For more information on SETA programs see also Appendix 2 – 7.

Besides the investigation of awareness raising methods, other ISA studies focus on the preceding role of ISA for ISS behavior. Diverse studies have proven ISA to be an essential direct and indirect determinant of ISP compliant behavior or intention respectively. For example, Galvez and Guzman (2009) identified ISA as one of the shaping factors of behavior and consider that "… the higher the information security awareness, the higher the information security practice" (p. 4). The general deterrence theory (GDT), originating from criminology research, recently has received the most attention to assess how IS misuse can be prevented or avoided (e.g., Straub and Nance, 1990, Lee and Lee 2002, D'Arcy and Hovav 2007a, 2007b, D'Arcy et al., 2009, Siponen and Vance 2010). The theory relies on threats as a deterrence effort and the actor's perceived certainty and severity of potential sanctions. Applying the GDT, D'Arcy et al. (2009) show that a high level of employees' awareness of organizational ISS countermeasures (e.g., SETA programs, computer surveillance, and ISPs) reduces IT misuse behavior indirectly, by increasing the employee's perception of the severity of sanctions and perceived certainty that IT misuse will be revealed. Siponen and Vance (2010) replenish these findings and show that invoking neutralization techniques and rationalizing (e.g. refusal of responsibility and guilt, blame from others, or compensation of harmful behavior with creditable behavior) can reduce the deterrence effects of informal sanctions. They also note that neutralization techniques are rather utilized by

employees of organizations with less distinctive security culture norms. By making use of the protection motivation theory (PMT) (Rogers 1975, 1983) and the theory of planned behavior (TPB) (Ajzen 1991, Fishbein and Ajzen 1975), Anderson and Agarwal (2010) state that being aware of security threats influences the employees' perception of the severity and probability of the threat, which are weighed against their beliefs in the efficacy of their actions, ultimately influencing their security behavior. Based on the technology acceptance model (TAM) (Davis 1989) and the TPB, Dinev and Hu (2007) found that the user's awareness of potential risks and threats of harmful technologies is a determining factor of their intention to make voluntary use of preventive information security technologies, such as anti-spyware software. Bulgurcu et al. (2010) studied the antecedents of employees' policy compliance, investigating the role of ISA on the outcome beliefs (1) perceived benefit of compliance, (2) perceived cost of compliance and (3) perceived cost of noncompliance and attitude towards intention to comply. They found significant effects of ISA on the three outcome beliefs and attitude. Shedding a light on the mediating effect of attitude on the relationship between ISA and intention, they found that attitude is only a partial mediator. Hence, a direct effect of ISA on the intention to comply with security policies is hypothesized. Intention is used in order to substitute actual behavior, since it "…is the most proximal influence on behavior and mediates the effect of other determinants on behavior" (Venkatesh and Brown 2001).

Hypothesis 1: ISA positively influences employees' intention to comply with the ISPs.

3 Antecedents of Information Security Awareness

To capture the different facets preceding ISA, the proposed research model incorporates variables related to ISS management practices and social psychology to address individual, institutional and socio-environmental determinants of ISA.

3.1 Institutional Antecedents of ISA

Institutional antecedents refer to an organization's security management practices. In the ISS literature, these factors are often summarized under the term "management support" (Chan et al. 2005). The greater the management support, the more resources are available for security issues (Kankanhalli et al. 2003, Herath and Rao 2009b). Scholars have emphasized that reasonable resources for security management are essential for establishing sufficient levels of security awareness among employees (Tsohou et al. 2009). Reviewing the ISS literature carefully, SETA programs and information security policy provision (ISP provision) are identified as vital institutional factors that can have an impact on employees' ISA.

3.1.1 Information Security Policy Provision

The development of corporate ISPs is a primary resource of ISS management practices (Chan et al. 2005). A policy in general is defined as ''a course of action, guiding principle, or procedure considered expedient'' (Houghton Mifflin. 2000). In the context of organizational information security, an ISP can be broadly defined as statements by an organization providing guidance about ISS related responsibilities, rules, and guidelines which prescribe how the IS resources are used properly and in a secure way (Whitman et al. 2001, Whitman 2008, D'Arcy et al. 2009).

Prior research offers contradicting results with regard to the effect of ISPs. While many studies found corporate ISPs to be effective for preventing IS misuse behavior, others revealed that the existence of an ISP had only limited influence on ISS related behavior. D'Arcy et al. (2009) for example, found corporate ISPs to be effective for preventing IS misuse behavior in organizations, and ascribed this effect to deterrence mechanisms of ISPs comparable to the mechanisms of societal laws. Similarly, Straub and Nance (1990) discovered policies and guidelines that specify rules for proper use of information

systems to be one of the security management's most effective deterrence measures against computer abuse. Kwon and Johnson (2011) gathered qualitative and quantitative data from IT managers of 250 healthcare organizations, and found that IS security policies were positively associated with the security performance of the organizations. Conversely, the literature also provides studies in which ISPs could not be proved to positively influence information security behavior (Foltz 2000, Wiant 2003, Lee et al. 2004). Such inconsistent results, the literature argues, are due to employees' lack of awareness of security policies (Thomson and von Solms 1998, Siponen 2000).

In this respect, scholars emphasize that the "simple" existence of ISPs is not enough, and highlight the importance of promoting ISPs and ensuring that they are comprehensible, easily available, and understandable. These aspects for effectively promoting ISPs are summarized here under the term ISP provision. There is broad empirical evidence that ISP provision is positively associated with security related behavior. For example, Chan et al. (2005) found that making ISPs readily available for employees' reference, as part of security management practices, is positively associated with their policy compliance behavior. Similarly, Siponen et al. (2009) found that the visibility of policies plays an important role in employees' compliance with organizational security policies. Herath and Rao (2009b) also showed that ISPs should be made easily accessible and available to employees online, and should furthermore be written in a clear and understandable way, as this has positive effects on the intention to comply. However, none of these studies investigated ISA. Based on the definition of ISA, it is claimed in this thesis that the reported positive direct effects of ISP provision on behavioral intention are largely a result of an increase in employees' awareness regarding ISP, and therefore also of security issues in general. This argument is consistent with the notion of D'Arcy and Hovav (2007b), who state that to enhance the individual's awareness of security policies, these should be available online and phrased in a manner that is easy to understand. The rationale employed here is that promoting easily accessible and comprehensible ISPs firstly raises employees' contextual awareness and knowledge, and secondly the situational intention to comply. Accordingly, it is contended in this study/thesis that ISA at least partially mediates the positive effect of ISP provision on security compliant behavior. Hence,

Hypothesis 2a: ISP provision positively influences employees' level of ISA.

Hypothesis 2b: ISA mediates the positive effects of ISP provision on the intentions to comply with ISPs.

3.1.2 SETA Programs

The mere existence of an ISP does not guarantee that employees internalize and comprehend it (Whitman 2003, Herath and Rao 2009a). Thus, once an organization has developed an ISP, its content, rules and specifications need to be communicated and trained throughout the organizations' employees and IS-users (Rotvold 2008). Institutional security education, training, and awareness raising programs typically referred to as SETA programs are the most important and qualified instrument for this purpose, and accordingly are one of the major ISS management resources (e.g., Chan et al. 2005, Puhakainen 2006, D'Arcy et al. 2009). In praxis and in the literature there exists a great variety of different designs, methods, and nomenclatures of institutional security training activities. Some of the various practices are e.g., the explanation of ISPs (Straub and Welke 1998), periodic newsletters, emails and presentations concerning ISS relevant issues (Spurling 1995, Herath and Rao 2009a), ISS workshops and seminars (Thomson and von Solms 1998), providing posters, flyers, and lectures (Crossler and Bélanger 2006), supporting online- and computer-based learning (Chen et al. 2006), or periodic security refresher courses (Hansche 2001a, von Solms and von Solms 2004). SETA programs aim to improve organizational information security by increasing employees' knowledge and awareness of potential security risks, policies, and responsibilities. Furthermore, they aim at providing employees with the skills necessary to comply with organizational ISS procedures (Straub and Welke 1998, Whitman et al. 2001, Lee and Lee 2002, D'Arcy et al. 2009). Thus, SETA programs intend to sensitize employees to the value of ISS, as well as to qualify them for security conscious use of organizational information resources.

Several studies provided evidence that SETA programs are an essential building block of security management and that they influence information security behavior positively. For example, Straub and Welke (1998) and Chan et al. (2005) empirically proved that SETA programs, being part of security management practices, lead to greater intentions

on the part of employees to comply with ISPs. Jenkins et al. (2010) designed an experiment which showed that training videos significantly increased employees' security password policy compliance. Other studies argue that SETA programs promote an individual's self-efficacy or perceived behavioral control regarding a related topic (Bandura 1989), which have been frequently proven to be essential prerequisites of ISS behavior (Lee et al. 2008, Ng et al. 2009, Jenkins et al. 2010, Herath and Rao 2009b, Bulgurcu et al. 2010). Other studies based on GDT argue that SETA programs communicate the presence of sanctions for policy violations, and therefore have a significant influence on employee security behavior by improving their perception of the certainty and severity of those sanctions (Straub and Welke 1998, D'Arcy et al. 2009). In addition, scholars emphasize the role of SETA programs on employees' ISA (e.g., Straub and Welke 1998, D'Arcy et al. 2009). Siponen et al. (2009) state that security education helps employees to become aware and develop an interest in security issues. They also contend that SETA Programs raise employees' consciousness about the vulnerability of their organization owing to ISS threats. As the primary goals of SETA programs are on ISS education, training, and awareness it is contended here that these programs have a positive impact on ISA and that the influence on intention to comply is at least partially mediated by ISA. Thus,

Hypothesis 3a: The provision of SETA programs positively influences employees' level of ISA.

Hypothesis 3b: ISA mediates the positive effects of SETA programs on the intention to comply with ISPs.

3.2 Individual Antecedents of ISA

3.2.1 Information Systems Knowledge

The rapid development of computer and online applications in recent years has caused a general increase in job requirements concerning IT skills in diverse professional fields (Choi et al. 2010). This study refers to IS knowledge as general knowledge of basic IS applications used in daily business, such as computers, email systems, and the Internet. Research indicates that there is a positive relationship between computer skills and ISS

related behavior (Frank et al. 1991). Dinev and Hu (2007) found that a higher level of technological awareness, also defined as IS knowledge, has a positive impact on the use of preventive ISS technology, such as anti-spyware software. Gaston (1996) states that an organization's IT staff possesses more IS knowledge than the employees in other departments, and thus have a higher level of awareness of possible ISS risks. In a quantitative survey, Rhee et al. (2009) showed that the respondents' level of computer- and internet-related knowledge and experience had a positive impact on security behavior. Conforming with these findings, it is believed that someone who has profound general IS knowledge and the ability to properly use the basic IS applications of daily business such as computers, email systems, and the Internet, is more aware about ISS related threats and potential risks appearing in these applications. It is hypothesized that IS knowledge affects awareness directly through its knowledge dimension and that the influence on intention to comply is at least partially mediated by ISA. Thus,

Hypothesis 4a: IS knowledge positively influences employees' level of ISA.

Hypothesis 4b: ISA mediates the positive effects of general IS knowledge on the intention to comply with ISPs.

3.2.2 Negative Experience

Employees may have directly or indirectly been harmed by any kind of ISS incidents such as worms, viruses, or phishing attacks either in private or working contexts. ISA may be shaped by such experiences, as negative incidents raise consciousness in the future, as well as interest in knowing how to prevent such incidents. Bulgurcu et al. (2010, p. 533) accordingly state life experiences "… such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations." may increase an individual's level of ISA. Therefore, it is hypothesized here that individuals who have been negatively affected by ISS incidents, either personally or indirectly, are more aware of information security issues. It is further claimed that the expected positive impact of negative experiences on security behavior is compensated by the negative effect on actual security behavior arising from a perceived loss in the ability to ensure ISP compliant behavior due to negative experiences (Rhee et al. 2009). Hence, only the following hypothesis is postulated:

Hypothesis 5: *Negative experiences with ISS incidents positively influence employees' level of ISA.*

3.3 Environmental Antecedents of ISA

Theories in behavioral research (Fishbein and Ajzen 1975) and social psychology (Fulk et al. 1987) highlight that individual behavior is always embedded in social contexts and, thus, is susceptible to interactions with one's social environment. The social environment can be separated into the influence of primary sources i.e. close peers, such as family members, friends, or co-workers and that of secondary sources, such as the mass media (Brown and Venkatesh 2005).

3.3.1 Secondary Sources' Influence

Research has shown that information received from secondary sources, such as the media, has an impact on individual behavior (Ajzen 1985, Brown and Venkatesh 2005, Rogers 1995). For example, mass communication and informational campaigns were found to positively influence society's waste recycling behavior (Chan 1998) and to reduce illicit behavior, such as workplace drug use (Quazi 1993). Also, several studies in the ISS domain suggest that individuals' understanding of security threats and their security behavior are positively related to information received from newspapers, journals, television, or the Intra- or Internet (NG and Rahim 2005, Siponen et al. 2009). Furnell (2006) contends that information related to ISS in the media can have an impact on the public awareness of information security issues. Consistent with this assumption, scholars state that employees' ISA may be built from external sources, such as the Internet, newspapers, or security journals (e.g., Bulgurcu, et al. 2010, Al-Omari et al. 2011). It is argued here that the positive impact of mass media coverage concerning ISS threats on recipients' ISA is largely due to increased interest in and knowledge of information security. The theory of planned behavior (TPB) (Ajzen 1991) argues that normative influences directly influence behavior. Hence, it is hypothesized that, given the effect of secondary sources' influence on individual consciousness and knowledge, the direct impact of secondary sources on intention is at least partially mediated by ISA. Thus,

Hypothesis 6a: Information about ISS from secondary sources positively influences employees' level of ISA.

Hypothesis 6b: ISA mediates the positive effects of secondary sources' influence on the intention to comply with ISPs.

3.3.2 Peer Behavior

The TPB (Ajzen 1991) highlights the impact of subjective norms upon individuals' behavior in organizations. This motivating effect can largely be ascribed to a human's desire for approval from significant others. But it is not only certain expectations from others that influence human behavior. It is also the exemplified behavior of relevant reference groups or persons that do so (Ajzen 1991). This motivational effect of observed peer behavior results from the fact that humans tend to think "…if everyone is doing it, it must be the sensible thing to do…" (Cialdini et al. 1990, Herath and Rao 2009a).

Also the context of ISS research, empirical evidence shows a positive impact of ISP compliant behavior of peers on the security behavior of others (Herath and Rao 2009a). It has also been shown that direct supervisory security practices and direct co-workers socialization, including conversations and the observation of the behavior of co-workers increase an employee's attention for organizational ISPs, which in turn positively affects security compliant behavior (Chan et al. 2005). Moreover, if co-workers disapprove ISP violations, employees are found to be less likely to do so (Siponen and Vance 2010). In addition, in the private context, it could be empirically proven that family members and peers significantly affect users' intentions to behave responsibly with regard to computer security (NG and Rahim 2005). Thus, there is strong evidence that peers affect employees' security behavior. However, it is argued in this study that interactions with peers initiate knowledge transfers (Spears 2006) and consequently increase ISS-related knowledge. It is therefore contended that ISP compliant peer behavior firstly increases ISA through its knowledge dimension (Leach 2003), and the direct effect of peer behavior is at least partially mediated by ISA. Hence,

Hypothesis 7a: ISP compliant peer behavior positively influences employees' level of ISA.

Hypothesis 7b: ISA mediates the positive effects of ISP compliant peer behavior on the intentions to comply with ISPs.

3.4 Proposed Research Model

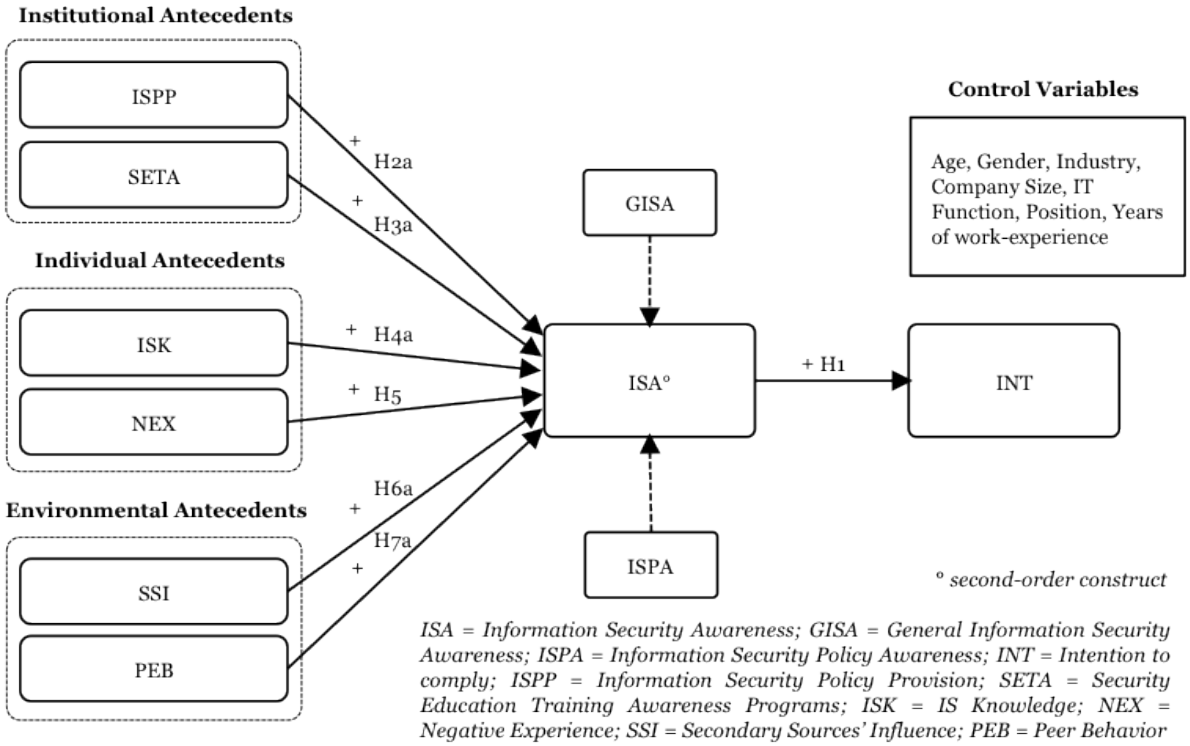


Figure 12: Proposed Research Model

4 Research Methodology

To validate the underlying model, quantitative survey method and structural equation modeling applying the component-based partial least square (PLS) approach were used. In the forthcoming section, the used measurement instrument and the sample of the study are exemplified.

4.1 Measurement Instrument

Standard psychometric scale development procedures were employed. When possible, validated scales were applied, but two measures, IS knowledge and ISP provision, were adapted to the context of the study. To validate these measures, qualitative and quantitative pilot studies were conducted, including sorting procedures with subsequent interviews of four practitioners and six scholars (Moore and Benbasat 1991). The dependent variable ISA was operationalized as a second-order construct, composed of the two first-order constructs general ISA (GISA) and ISP awareness (ISPA) (Bulgurcu et al. 2010). GISA corresponds to an individual's overall knowledge and understanding of ISS issues and their potential consequences, while ISPA refers to the knowledge and understanding of the requirements of the organization's ISPs (Bulgurcu et al. 2010). Aside from the items of negative experience, all items were assessed on seven-point Likert-scales ranging from "strongly disagree" (1) to "strongly agree" (7) (Likert 1932). Following the suggestions of prior ISS research to include extraneous control variables that potentially may influence ISS security behavioral aspects, recipients were asked for demographic characteristics, such as age, gender, working experience, and whether or not they work in an IT function. Additionally, it was controlled for company size and type of industry. For practicability reasons and time restrictions of the survey method, only the four industry types were included that are known to be most critical and vulnerable for ISS incidents, namely "financial services", "consulting", "manufacturing", and "information technologies and telecommunication".

The study incorporates both reflective and formative measurement scales. Whereas the variables ISP provision and SETA programs were modeled as formative measures based on the criteria specified by Jarvis et al. (2003) and consistent with the original measures, all other variables were measured with reflective scales. Formative constructs are

generated from indicators that represent independent and different dimensions, whereas reflective items are all from the same dimension of a single underlying concept. This means that a change in the indictors of a formative measurement model should cause changes in its associated concept of the construct. On the contrary, adding or deleting indicators of a reflective construct should not have any essential consequences for the underlying concept. Formative items do not necessary covary with each other and their causality is always directed towards the construct and not the other way round, such as within reflective measures (Jarvis et al. 2003).

All original items were initially formulated in English and were subsequently translated into German. To ensure that the meanings between the original and the translated measures remained the same, native speakers in both languages translated them back into English and checked if the items were consistent with the original items. After some small adjustments of the translations, no more significant differences between the German and English versions existed, assuming to have a proper translation of the measurement instrument. Before going into the field, the survey instrument was pre-tested to ensure the initial reliability of the scales and clear unambiguousness of the questions, and further to check for general mechanics of the questionnaire, such as survey instructions, completion time, and the ease of understanding of the wording. An initial online questionnaire, including a feedback comment function for each item, was subjected to 19 people. Among those, 10 people had profound experience in quantitative research methods. Additionally, feedback from the study's target group (employees in organizations) was gathered to receive realistic and impartial answers and comments. Based on the first pre-test, the order and wording of some items were revised. After pre-testing a second round, the measurement instrument was proven to consist of clear and understandable items and distinguishable constructs. The final 28 items of the latent variables along with their sources, type of scales, and factor loadings are outlined in Table 15.

Construct (Source)	Items	Scale	Type	Factor Loading
Intention to Comply (Bulgurcu et al. 2010)	1_I intend to comply with the requirements of the ISP of my organization in the future.	a	r	.969***
	2_I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	a	r	.947***
	3_I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	a	r	.961***
General Information Security Awareness (GISA) (Bulgurcu et al. 2010)	1_Overall, I am aware of the potential security threats and their negative consequences.	a	r	.896***
	2_I have sufficient knowledge about the cost of potential security problems.	a	r	.772***
	3_I understand the concerns regarding information security and the risks they pose in general.	a	r	.821***
Information Security Policy Awareness (ISPA) (Bulgurcu et al. 2010)	1_I know the rules and regulations prescribed by the ISP of my organization.	a	r	.935***
	2_I understand the rules and regulations prescribed by the ISP of my organization.	a	r	.903***
	3_I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.	a	r	.931***
Information Security Policy Provision (ISPP) (Chan et al. 2005, Herath and Rao 2009b)	1_Information Security policies are made available to employees online.	a	f	-.023
	2_ISPs are written in a manner that is clear and understandable.	a	f	.652***
	3_Corporate ISPs are readily available for my reference.	a	f	.421***
Security, Education, Training, and Awareness (SETA) Programs (D'Arcy et al. 2009)	1_My organization provides training to help employees improve their awareness of computer and information security issues.	a	f	-.031 †
	2_My organization provides employees with education on computer software copyright laws.	a	f	.155**
	3_In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	a	f	.601***
	4_My organization educates employees on their computer security responsibilities.	a	f	.386***
	5_In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	a	f	.151 †
IS Knowledge (ISK) (adapted from Bassellier et al. 2003)	1_What is your general knowledge of personal computers?	b	r	.910***
	2_What is your general knowledge of the Internet?	b	r	.926***
	3_What is your general knowledge of email-systems?	b	r	.932***
Negative Experience (NEX) (Rhee et al. 2009)	1_Have you ever had problems because of a virus on your computer during the last two years?	c	r	.872***
	2_Have you ever had spyware on your computer during the last two years?	c	r	.794***
Secondary Sources' Influence (SSI) (Brown and Venkatesh 2005)	1_Information from mass media (TV, radio, newspapers, internet) suggest that I should comply with the ISP of my employer.	a	r	.863***
	2_Information that I gather by mass media (TV, radio, newspapers, internet) encourage me to comply with the ISP of my employer.	a	r	.954***
	3_Based on what I have heard or seen on mass media (TV, radio, newspapers, internet), I am encouraged to follow the ISP of my employer.	a	r	.949***
Peer Behavior (PEB) (Herath and Rao 2009a)	1_I believe other employees comply with the organization ISPs.	a	r	.949***
	2_I am convinced other employees comply with the organization ISPs.	a	r	.919***
	3_It is likely that the majority of other employees comply with the organization ISPs to help protect organization's information systems.	a	r	.910***

* p < .05; ** p < .01; *** p < .001; † removed items; Scale a: Seven-point Likert scale: (1) “strongly disagree” –(7) “strongly agree”; Scale b: (1) “no general knowledge at all” – (7) “very good general knowledge”; Scale c: (1) = No; (2) = Yes; Type r = reflective; f = formative.

Table 15: Measurement Items and Item Loadings

4.2 Sample and Data Collection Procedure

The proposed research model was validated with data collected in an online survey in October 2012, in Germany, using the pre-tested measurement instrument as presented in Table 15. For the technical realization of the survey, the online-survey-tool "www.soscisurvey.de" was applied which is commonly known among German researchers for its good usability. A web-based survey instrument seemed to be adequate, since the recipients were exclusively employees who use IS and have internet-access at their organization. Employees from a diverse set of organizations were recruited by spreading the questionnaire-links throughout multiple distribution channels. First, the link to the questionnaire was sent to a broad list of single business contacts (about n=250) and multiplier-contacts (about n=50) of my private network and the network of my colleagues and professors. Multiplier-contacts thereby were defined by people being in an executive management position with the chance to forward the link to colleagues and other employees of their organization. Second, different alumni-mailing-lists were used to spread the link, such as a list consisting of over a thousand "CDTM alumni" (Center for Digital Technology and Management, an institution for students of the LMU and TU in Munich), "e-fellows.net" (about 1,200), "Academy Consult e.V." (about 500), and a trainee-alumni list of "Siemens AG" (about 250). Third, the link was posted on the wall of over forty different business-network groups of the German business network "XING.com", whereas these groups were properly diversified concerning their respective industries. To increase the response rate, all participants were incentivized through a lucky lottery and were offered the chance to receive the results of the study on demand.

Over the sample period from 15th October 2012 through 15th November 2012, the survey website was visited 1,120 times, resulting in 661 completely finished questionnaires. From this sample respondents who were self-employed (n = 64) and whose employers did not have explicit ISPs were excluded (n = 59). Following Bulgurcu et al. (2010), these two exclusion criteria were applied because the study aimed to survey employees of organizations, and because the dependent variable "ISA" was partially constructed by the employee's awareness of their organization's ISPs. From the remaining dataset, questionnaires with an implausibly short handling time (t < 250

seconds) were screened out to avoid untrustworthy click-through answers (n = 38). The average response time for a fully completed questionnaire was 520 seconds. A rough examination of the plausibility of several response schemes resulted in an elimination of further 24 cases. Finally, one questionnaire was excluded because its recipient declared "0" to be his age. Because a successful completion of the survey was only possible by answering every single question, missing values could be avoided. After all of these clearing efforts, the final sample consisted of 475 completed and useable questionnaires.

Of the remaining 475 participants in the final sample, 68% were female, and the average age was 35.3 years, ranging from 20 to 67 years. Respondents that reported working for companies in the "IT industry (information technologies and telecommunication)" represented the largest share of the sample (25.8%). This was followed by "manufacturing" (9.8%), "consulting" (8.4%), and "financial services" (6.2%). 16.2% of the participants reported to work in IT functions of their organizations. The sample was quite evenly distributed with regard to the recipients' years of work-experience, which had an average of 10.8 years. Last, but not least, the sample consisted of quite similarly sized proportions of employees from small, medium-sized, and large companies, ranging from less than 100 to more than 9,999 employees. A detailed illustration of all sample demographics is presented in Table 16.

Before beginning the main analyses, the data was furthermore checked for a possible non-response bias, as recommended by Armstrong and Overton (1977). In this regard, no significant differences were exhibited between the first and the last third of the data set, assuming that non-response bias was not a problem. In summary, the final sample represented a diversified set of employees with different backgrounds, working at a broad bandwidth of small to large organizations from multiple industries. This heterogeneity of the sample is considered to be one of the study's strengths, since it may reduce the potential bias, resulting from influences through unique organizational factors, such as policy matters or corporate cultural aspects, when dealing with a small number of organizations (Bulgurcu et al. 2010).

	n = 475	100%
Gender		
Male	323	68.0%
Female	152	32.0%
Age		
Min	20	
Max	67	
Mean	35.52	
20-25	40	8.4%
26-35	248	52.2%
36-45	113	23.8%
46-55	59	12.4%
56-65	13	2.7%
66 and over	2	.4%
Industry		
Consulting	40	8.4%
Financial Services	29	6.2%
IT and Telecommunication	123	25.8%
Manufacturing	46	9.8%
Others	237	49.8%
IT Job Function	77	16.2%
Work Experience		
Min	0	
Max	46	
Mean	10.81	
< 2 years	66	13.9%
3-5 years	129	27.2%
6-10 years	96	20.2%
11-15 years	69	14.5%
16-20 years	36	7.6%
> 20 years	79	16.6%
Company Size		
Less than 100 Employees	87	18.3%
100-499	112	23.6%
500-999	31	6.5%
1.000-2.499	42	8.8%
2.500-9.999	70	14.7%
More than 9.999	133	28.0%

Table 16: Demographics of Participants

5 Data Analysis and Results

As mentioned before, the research model was validated using structural equation modeling. The component-based partial least square (PLS) approach was chosen using SmartPLS version 2.0.M3 (Ringle et al. 2005).

The PLS method has become increasingly popular in diverse research areas in recent years (Hair et al. 2012), especially because it leads to robust results with few methodological requirements. Alongside marketing, economics, and behavioral research, PLS has also been preferably applied for behavioral ISS studies in several highly ranked IS journals (e.g., D'Arcy et al. 2009, Bulgurcu et al. 2010, Siponen and Vance 2010). PLS was considered to be appropriate for this study because of four main reasons. First, PLS as a component-based approach is the best method to use if the underlying model is rather exploratory and not based on a prevalent and often validated theory. Nevertheless, the development of the causal model cannot simply be data-driven, but rather requires a proper theoretical-based derivation of the hypotheses and measurement operationalizations (Diamantopoulos et al. 2008, Gudergan et al. 2008). Second, it does not premise a normal distribution of data of any of the indicators and variables (Chin and Newsted 1999). Third, PLS does not mind the types of scales and is able to manage reflective and formative measurement scales, both used in this study (Jarvis et al. 2003). Finally, PLS as a component-based approach estimates the elements of the measurement and structural model partially, and therefore places minimal restrictions on the size of the sample (Chin and Newsted 1999).

The next two chapters describe the data analysis which followed the two-stage procedure proposed by Anderson and Gerbing (1988). In the first stage, the psychometric properties of the reflective and formative measurement models are assessed using standard quality criteria proposed in the literature. In the second stage, the research hypotheses are tested, by estimating the inner structural model.

5.1 Assessment of Measurement Model

The study incorporates reflective and formative measurement scales. Since formative constructs cannot be assessed using the same reliability and validity tests as reflective constructs, they were evaluated separately (Diamantopoulos and Winklhofer 2001).

5.1.1 Quality of Reflective Measures

To assess the reflective variables, reliability and validity tests were conducted according to the guidelines of Gefen and Straub (2005). First, individual item reliability was examined to approve if the respective items qualified as indicators for the underlying constructs (Johnson et al. 2006). As illustrated in Table 15, all reflective items loaded significantly on the underlying constructs, with values well above the recommended threshold of .707 (Chin 1998), and none of the items loaded on their construct below the cutoff value of .50, suggesting that at least 50% of the single indicators' variance could be linked to the respective latent variables (Johnson et al. 2006). In the next step, it was checked for adequate construct reliability (CR), using composite reliability scores that result from PLS internal consistency scores. The CR shows how consistently the constructs are represented by their respective indicators, and how free they are from random error (Chin 1998). Bagozzi and Yi (1994) suggest the value of CR to be at least higher than .60, whereas the majority states .70 to be the critical value (Nunnally 1978, Fornell and Larcker 1981, Gefen and Straub 2005). As shown in Table 17, all CR values exceeded both of the recommended thresholds. In addition to that, Cronbach Alpha (CA) values were calculated. All CA values exceeded the suggested minimum value of .70 (Chronbach 1951), also indicating that poor construct reliability was not an issue in this study. Hence, reliability tests indicated that indicator and construct reliability were well developed.

Convergent validity was assessed by examining the constructs' average variance extracted (AVE) and the individual item reliability. As illustrated in Table 17, results show that the AVE score of each construct was well above the common threshold of .50 (Bhattacherjee and Premkumar 2004) and item reliability was given as examined before. Hence, convergent validity was confirmed. To establish discriminant validity, the criterion of Fornell and Larcker (1981) was applied and a confirmatory factor analysis was conducted to check cross-loadings (Appendix 9). The correlations between any two constructs were lower than the square root of the corresponding AVE (Fornell and Larcker, 1981), and the indicator items loaded more strongly on their corresponding construct than on any other construct (Gefen and Straub 2005). Hence, the required criteria for discriminant validity were met successfully.

The applied reliability and validity tests showed very satisfying results. All items of the reflective measurement model, as presented in Table 15, were used to test the structural model.

Variable	Range	Mean	SD	CR	CA	AVE	INT	GISA	ISPA	NEX	ITK	SSI	PEB
INT	1-7	6.06	1.04	.971	.968	.921	**.963**						
GISA	1-7	5.56	1.12	.870	.774	.691	.403	**.831**					
ISPA	1-7	5.48	1.32	.946	.913	.853	.521	.593	**.924**				
NEX	1-2	1.28	.37	.820	.665	.695	-.072	.030	.035	**.834**			
ISK	1-7	5.48	1.32	.945	.913	.851	.167	.377	.320	-.072	**.922**		
SSI	1-7	4.67	1.62	.944	.914	.848	.351	.283	.227	-.023	-.028	**.921**	
PEB	1-7	4.78	1.44	.947	.917	.857	.443	.272	.416	-.103	.016	.287	**.926**

SD = Standard Deviation; CR = Composite Reliability; CA = Cronbach Alpha; AVE = Average Variance Extracted; INT = Intention to comply; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; NEX = Negative Experience; ISK = Information Systems Knowledge; SSI = Secondary Sources' Influence; PEB = Peer Behavior; bold diagonal elements represent the square root of AVE; CA, CR, AVE cannot be computed for formative measures.

Table 17: Composite Reliability, AVE, Latent Variable Correlation

5.1.2 Quality of the Formative Measures

Although these are rather rare methods to test for reliability and validity of formative scales, it was proceeded with the following using steps suggested in the literature to assess the quality of the two formative constructs SETA programs and ISP provision.

First, item weights were checked to identify their relevant importance for their underlying constructs. It is recommended that the indicator weights exceed the value of .20 and are significant (Chin 1998). The item weights of SETA_1 (-.031), SETA_5 (.151) and ISPP_1 (-.023) were under this threshold and not significant, thus it was recommended for them to be dropped. As illustrated in Table 15, all other formative item weights were significant at the .01 level or better and loaded higher than the threshold of .20 on their underlying latent variable. Before removing any item, the literature suggests considering whether or not the elimination would harm the content validity of the construct (Diamantopoulos and Winklhofer 2001). The construct SETA programs was represented by 5 items, which all aimed to inquire similar dimensions concerning the information security training endeavors of the recipient's organization. The items SETA_1 and SETA_5 were captured more generally in their corresponding construct and therefore it could be assumed that an elimination of theses items would

not change the construct's concept (D'Arcy et al. 2009). Additionally the structural model was tested twice with and without the removed items. No significant differences were reported. For these reasons the two indicators of SETA programs were excluded from all following analyses. The item ISPP_1 represented the online availability of ISPs and was a selective dimension of the concept of policy provision. To ensure content validity, it was decided to remain this indicator for all remaining analyses.

Second, to further examine convergent and discriminant validity of the remaining formative indicators, a "weighted item-to-construct matrix" was created as presented in Table 18, following Loch et al (2003). Therefore, item scores were multiplied by their PLS weights and subsequently summed up to get the weighted composite score for each formative construct (Cal_SETA and Cal_ISPP). All weighted items correlated significantly at a .01 level against the composite score for their corresponding construct, indicating that convergent validity of the measures was successfully given (Loch et al. 2003). To check for discriminant validity, Loch et al (2003) suggest that each indicator's weighted score should correlate higher with its own construct than with the composite score of any other formative constructs. As this condition was fulfilled (see Table 18), improper discriminant validity seemed not to be an issue for the formative scales.

As a last step, it was tested for multicollinearity as suggested by Diamantopoulos and Winklhofer (2001). In contrast to reflective measures, formative constructs suffer from the existence of multicollinearity within the scales because this can destabilize their measurement model (Jarvis et al. 2003). Therefore the variance inflation index (VIF) was calculated. A series of regression models were carried out among all items of each construct, whereas each item served one time as the dependent variable, loaded on by all other items of the construct. The resulting R^2 for each dependent item was then used to calculate the VIF, following Glenn et al. (2006). High multicollinearity can be suspected when the value of VIF is over the common cutoff level of 10.0 (Diamantopoulos and Winklhofer 2001). Even when applying the more conservative cutoff level of 5.0 (Hair et al. 1998), it could be shown that multicollinearity seemed not to be a problem. As presented in Table 18, all VIF values were below the claimed threshold.

Construct	Weighted scores	Cal_SETA	Cal_ISPP	weights	T-value	VIF
SETA Programs	SETA_2	**0.948****	0.563**	0.532	3.815	3.46
	SETA_3	**0.781****	0.467**	0.259	2.782	1.72
	SETA_4	**0.928****	0.532**	0.315	2.304	3.80
ISP Provision	ISPP_1	0.451**	**0.557****	-0.023	0.487	3.78
	ISPP_2	0.536**	**0.940****	0.611	7.005	2.60
	ISPP_3	0.565**	**0.915****	0.479	4.853	3.63

Item scores were multiplied with their PLS weights and summed up to get the composite score Cal_Construct (Loch et al. 2003); ** Correlation is significant at the .01 level (2-tailed); VIF = Variance Inflation Index = $1/(1-R^2)$; To get the VIF, diverse regression models were conducted among all items of each construct. Thereby, each item served one time as the dependent variable and all other items of the construct as independent variable. The R^2 of each dependent variable was used to calculate the VIF, following Glenn et al. (2006).

Table 18: Weighted Item-to-Construct Matrix and VIF

5.2 Testing of Structural Model

Based on the refined measurement model, the research model was validated using structural equation modeling. The analysis included the estimation of standardized path coefficients and the amount of variance in ISA and intention (R^2). The significance of the coefficients was estimated by bootstrapping the 475 cases with 3,000 re-samples, as suggested by common IS literature.

The results show (see Figure 13) that all hypothesized direct effects of ISA's antecedents on ISA are supported (H2a, H3a, H4a, H5, H6a and H7a ($p < .05$). Results also confirm the positive effect of employees' ISA on the intention to comply with ISPs ($\beta = .30$, $p < .001$). The research model could explain for .50 of the variance in the variable ISA and for .40 of the variance in the variable intention to comply. These values can be considered as a good and nearly substantial value (Chin et al. 1998). The weights of the two sub-dimensions GISA (w1 = .466) and ISPA (w2 = .650) of the second order construct ISA were also significant ($p < .001$) indicating that each sub-dimension significantly contributes to the underlying overall factor. None of the control variables except working experience ($\beta = .094$, $p < .05$) and gender ($\beta = -.137$, $p < .001$) were found to be significant. It was also tested for common method bias, since independent and dependent variables were provided by the same respondent. Both, the Harman's single-

factor test (Podsakoff et al. (2003) and the marker variable test (Lindell and Whitney 2001) indicate that common method bias was not a threat to the validity of our study.

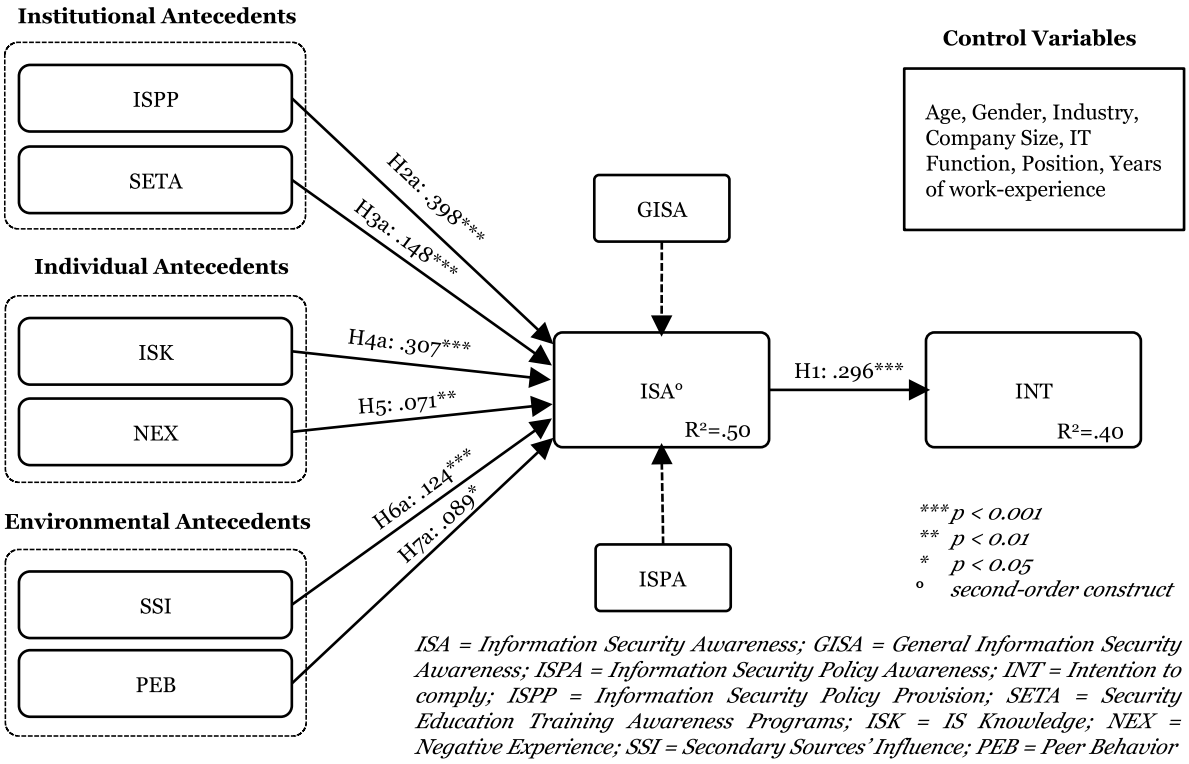


Figure 13: Results of Testing the Structural Model

5.3 Mediation Analysis

To test the hypothesized mediating role of ISA, the widely used procedure proposed by Baron and Kenny (1986) was performed. The results of the mediation analysis are summarized in Table 19. For supporting significant mediation according to Baron and Kenny (1986), the following four conditions need to be fulfilled (see Figure 14).

First, the considered independent variable (IV) must account for variations in the dependent variable (intention to comply), when not controlling for the mediator (ISA) (path c'). This condition is successfully met for each IV (p<.001). Second, the mediator must significantly account for variations in the dependent variable (path b). This condition is likewise fulfilled (ß = .296, p<.001). Third, the IV must significantly account for variations in the mediator (path a). This condition is satisfied for all IV's with (p<.001) and peer behavior (p<.05). Finally, the effects of the IVs on the dependent variables (path c') must decrease significantly when controlling for the mediator (path

c). The results suggest the existence of a full mediation, if path c' becomes statistically insignificant when controlling for the mediator (path c), and suggests a partial mediation, if path c' only decreases but path c still stays significant.

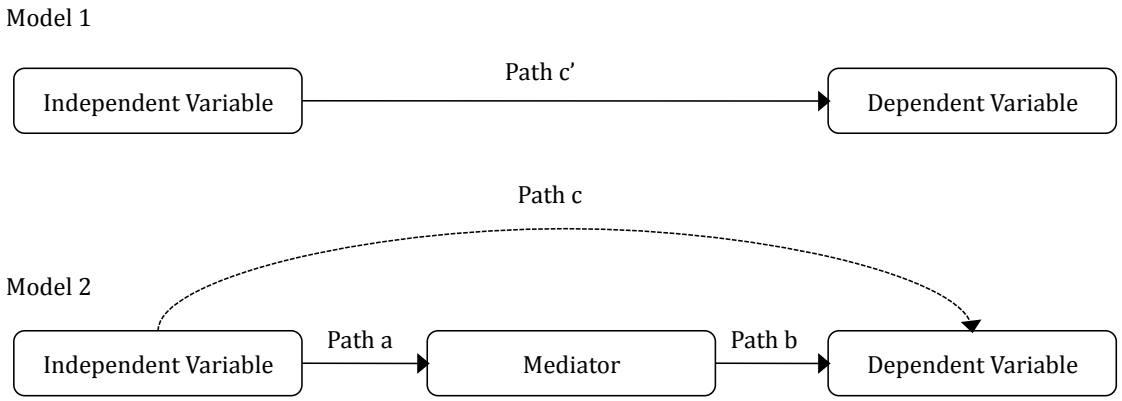


Figure 14: Paths in Mediation Models (Baron and Kenny 1986)

Whether or not the mediation effect is significant can be examined by Sobel's (1982) test of indirect effects. It is tested whether the effects of the independent variable drops significantly once the mediator is incorporated into the model. The results in Table 19 show that all mediation hypotheses were confirmed as all four conditions were met for each hypothesis. ISA fully mediates the effects of ISP provision and SETA programs on the intention to comply and partially mediates the effects of IS knowledge, secondary sources' influence, and peer behavior.

Hypotheses	IV	Model II			Model I	Sobel's Test	Mediation
		a	b	c	c'	z	
H2b	ISPP	.398***	.296***	.055	.166***	4.421***	Full Mediation
H3b	SETA	.143***	.296***	.069	.115***	2.639**	Full Mediation
H4b	ISK	.307***	.296***	.071*	.158***	4.24***	Partial Mediation
H6b	SSI	.124***	.296***	.167***	.203***	2.951**	Partial Mediation
H7b	PEB	.089*	.296***	.212***	.236***	2.069*	Partial Mediation

ISPP = Information Security Policy Provision, SETA = Security Education Training and Awareness Programs, ISK = Information Systems Knowledge; SSI = Secondary Sources' Influence; PEB = Peer Behavior; Model I: without controlling for the mediator (ISA); Model II: with controlling for the mediator; Path a: IV -> mediator; Path b: mediator -> intention; path c and c': IV-> intention; * p < .05; ** p < .01; *** p < .001.

Table 19: Mediation Analyses of ISA

6 Discussion

This study addresses an important gap in the information security literature regarding the emergence of employees' ISA. Understanding which factors influence ISA is crucial, since employees' awareness has been found to be a substantial determinant of ISP compliant behavior. In the present study a research model comprising institutional, individual and environmental antecedents of ISA is proposed and empirically tested. The model explains a substantial proportion of the variance in ISA (R^2 = .50). The findings have important implications for information security managers and researchers. The promotion and provision of ISPs is the most substantial antecedent of ISA. Thus, an effective, economic, and relatively easy way to make employees aware of information security issues is to provide policies which are understandable for all employees of an organization, and easily accessible on- and offline at any time. Although many scholars claim that SETA programs increase ISA, hitherto empirical evidence was limited. The results confirm the hypothesized positive effect of security trainings on ISA. Thus, an essential task of security and general management is to provide employees with suitable SETA programs. At the individual level, it was found that general IS knowledge is an essential predictor of ISA. The more employees know about IS, the more aware they are regarding ISS related issues. Therefore, organizations should seek to improve the skills of those employees lacking general IS knowledge to avoid unintentional misbehavior. Prior negative experiences with ISS incidents also had a positive - although smaller - effect on ISA, supporting the rationale that once someone has been affected directly or indirectly by incidents, the awareness of information security issues increases (Bulgurcu et al. 2010). To raise ISA, organizations may build on this finding by offering information on attempted and actual cyber-attacks on the organization, to point out the virulent threats of misbehavior. Also, information about ISS incidents from outside the organization should be communicated, as the study found that information provided by secondary sources also raises ISA. The same effect was found for the influence of peer behavior, however to a lesser extent. This finding was unexpected, as prior research suggests that the behavior of peers is an important antecedent of ISA. One reason for this might be that the ISS compliant behavior of peers is difficult to observe, and thus does not affect the individual ISA as strongly as the literature would suggest. The

significant effect of the control variables working experience and gender is also worth noting, as they indicate that female employees and employees with greater working experience have a significantly greater intention to comply with ISPs (see Appendix 10).

The mediation analysis reveals the significant role of ISA for ISS behavior. ISA was found to fully mediate the relationships between intention to comply and ISP provision and SETA programs. Additionally, ISA partially mediates the effects of IS knowledge, secondary sources' influence, and peer behavior on intention to comply. It can be theorized about the reasons for the full mediating effect of ISA between ISP provision and intention, and SETA programs and intention. ISA as defined by this study captures two dimensions, employees' general knowledge about information security and the cognizance of the employer's specific ISPs. ISP provision and SETA programs address both dimensions, and once ISA is established, the knowledge of general ISS-related issues and threats, as well as an organization's ISP, apparently become internalized by employees, hence a full mediation through ISA. These results underscore the vital role of employees' security awareness on security compliant behavior. ISA alone explains .40 of the variance in intention to comply. Hence, security managers must stay focused on ISA-building/maintaining levers. In relation to the environmental variables (negative experiences, secondary source influence, peer behavior) included in the research model, ISP provision, SETA programs, and IS knowledge have a stronger impact on intention through ISA. This is good news for ISS managers, as those variables can be influenced directly by organizations. Thus, the main resources of ISS managers should focus on an effective provisioning of comprehensible ISPs, offering of target-group specific SETA programs, and specifically addressing employees' IS skills shortages. Concentrating on those security countermeasures would also have a reinforcing effect on the relationships between normative influences (secondary sources' influence and peer behavior) and intention to comply, which are only partially mediated by ISA.

As with any other empirical study, this study has limitations that should be considered when interpreting the results. The first limitation is due to some characteristics of the sample. The data collection procedure was geographically confined to Western Europe. Hence, to generalize the findings, future research is needed to account for cultural differences which may be of particular interest for multinational organizations. The sample consisted only of employees whose organizations had developed explicit ISPs

because of the ISP dimension of the definition of ISA. This selection could have been responsible for a favorability bias in the data (Bulgurcu et al. 2010). Accordingly, an avenue for future research may be to investigate antecedents of ISA of employees including organization without explicit ISPs. Another limitation, and also an avenue for further research, is due to restrictions of the measurement instrument. The study had to rely on intention to comply as the dependent variable, instead of actual behaviors. Although literature contends that intention is the most proximal influence on behavior, there is no guarantee that employees will behave as indicated. Although there exists sound empirical support that employee's intentions to comply with ISPs have a significant impact on actual compliant behavior (Pahnila et al. 2007a), future research should reassess the research model measuring actual behavior. For the dependent variable ISA, perception-based measures were applied, which are generic. Because the data collection procedure was strongly limited with regard to answering time, it was not practicable to use an extensive and differentiated list of questions for a more objective measure of ISA and intention. To gain more objective insights into the development process of ISA, future research is needed – for example in the form of case studies – that investigate the antecedents of ISA in one or only few organizations using a more differentiated and objective measure of ISA. Another avenue for further research is to consider the effect of moral reasoning, since an individual's moral commitment has been found to influence IS misuse intentions (D'Arcy et al. 2009). Furthermore empirical studies should explore whether or not individual characteristics such as overall job attitude, job satisfaction and organizational commitment moderate the effectiveness of SETA programs in improving ISA, which has been proposed by Wipawayangkool (2009b) but has yet not been validated. Also, future research could delve deeper into the "black box" of SETA programs. In this respect, field experiments analyzing the security awareness of employees before and after SETA programs could substantially contribute to our understanding of the emergence of employees' ISA. Moreover, the cross-sectional design of the data limits the generalizability of the findings in at least two ways. First, with regard to information security, user perceptions may change significantly over time, e.g. because of contemporary incidents. Second, the posited causal relationships can only be inferred. Thus, future research should employ longitudinal research designs. Last, but not least, this study identified and tested two antecedents of the three

categories, institutional, individual and environmental. Future studies are suggested to aim to indentify and empirically test additional antecedents of ISA to gain more comprehensive insights into the explanation of ISA. Factors could be, for example, differences in personality traits, such as conscientiousness or agreeableness or the influence of the organization's information security culture, which all have already been proven to play a role for ISS behavior, and are potentially linked to ISA.

7 Conclusion

A key goal of research on information security is to identify and understand how managerially controllable antecedents influence employees' security awareness and behavior. This article provides important insights on the antecedents of ISA and its mediating role on the relationship between its antecedents and intention to comply with ISPs. The results provide evidence that several institutional, individual, and environmental factors that prior research has considered as direct antecedents of security behavior are in fact at least partially mediated by ISA. Thus, this study refines prior research and serves as a starting point for further research on the role of ISA on security compliant behavior.

E. Study III: Why Deterrence is Not Enough: The Role of Endogenous Motivations and Information Security Awareness on Employees' Information Security Behavior[3]

Abstract

Refining our understanding of how employees' behavior regarding information systems security (ISS) can be explained and influenced is a top priority in academia and business practice (D'Arcy et al. 2009, Siponen and Vance 2010). In this respect, numerous studies have examined the role of deterrence mechanisms, such as monitoring or sanctioning on individual security compliance. A perspective largely neglected by prior research is the role of endogenous motivations (Siponen and Oinas-Kukkonen 2007), although studies in adjacent fields have shown the effectiveness of motivational intervention strategies (Wunderlich et al. 2013). This study seeks to close this gap by examining how endogenous motivations influence individual ISS-related behavior. The proposed model integrates the theory of planned behavior (TPB), the organismic integration theory (OIT) – a sub-theory of the self-determination theory (SDT), and the concept of information security awareness (ISA). The model was empirically tested using a sample of 444 employees from different organizations. The results show that when employees' personal values and principles are congruent with their employer's ISS-related prescriptions and goals, their intention to comply with security policies significantly increases. On the contrary, no impact on compliance intention was found when employees perceive their actions as a result of external pressures and coercion. The model further confirms the essential role of ISA for ISP compliant behavior by showing its preceding role for endogenous motivations, attitude, and the intention to comply. The study's findings advance our understanding of the motivational processes underlying security compliant behavior and provide numerous implications for researchers and practitioners.

[3] An earlier version of this paper was presented at the International Conference of Information Systems (ICIS 2014) in Auckland, New Zealand, December 14-17, 2014.

1 Introduction

According to Norton Symantec Cybercrime Report (2013), 378 million people have been marred by cybercrime in the past year, causing estimated losses for organizations worldwide worth US $445 billion (The Economist 2014). The main reasons for security breaches are malicious attacks, system glitches, and mistakes by employees. For hackers, employees represent popular targets to intrude on a company's network, as it is estimated that around 20 percent of employees enter their usernames and passwords in response to faked phishing e-mails, which pretend to come from legitimate sources (The Economist 2014). Recent studies estimate that more than 50 percent of all ISS incidents in organizations are the direct or indirect consequence of employees' misbehavior (Ernst and Young 2005, Siponen and Vance 2010). On an average, a company loses US $277 for each user account put at risk. With the number of threats and the severity of their consequences increasing, avoiding information systems security (ISS) incidents is becoming a major challenge for organizations (Gordon et al. 2011). As a result, large companies reportedly spent more than $32.8 billion on ISS in 2012, according to International Data Corporation, a research firm (Chen et al. 2012a). Small- and medium-sized organizations are even expected to spend more on ISS than on other IS/IT over the next three years (Perlroth and Rusli 2012). The investments often focus on technological remedies, such as encryption, anti-spyware, virus detection, or firewalls (Spears and Barki 2010). However, without training employees in how to recognize malicious attacks and avoid unintentional errors, organizations cannot succeed in information security (Siponen 2000, Son and Rhee 2007, Boss et al. 2009, Bulgurcu et al. 2010). Although most companies regularly offer security education, training and awareness (SETA) programs to employees, the success of these programs is limited due to a lack of engagement and participation. Practitioners and researchers alike are thus interested in how to improve employee engagement and motivation to comply with organizational ISS guidelines (Siponen and Oinas-Kukkonen 2007, Bulgurcu et al 2010, Johnston and Warkentin 2010).

Numerous previous studies on ISS have focused on deterrence mechanisms to explain why employees do or do not adhere to information security policies (ISPs) (e.g., D'Arcy and Hovav 2007a, 2007b, D'Arcy et al., 2009, Herath and Rao 2009a and 2009b,

Workman et al. 2009, Siponen et al. 2006, 2010). These studies implicitly suggest that extrinsic motivations, e.g., avoidance of sanctions, are the major motivation for employees to comply with organizational security guidelines. Another stream of motivational ISS studies, which is largely based on protection motivation theory (PMT) (Rogers 1975, 1983), investigated intrinsic factors such as employees' perceived effectiveness of information security behavior, perceived intrinsic costs or benefits of ISP compliance (Bulgurcu et al. 2010), or the perceived mental pleasure of committing the intended act (Hu et al. 2011). However, traditional motivational studies predominantly followed mechanistic motivation theories, which contend that behaviors are either being triggered extrinsically by rewards or intrinsically when the activity itself is the reward (exogenous motivation). These studies have not differentiated between different forms of extrinsic motivation ranging from external to internal perceived locus of causality. Self-determination theory (SDT) and its sub-theory, the organismic integration theory (OIT), in contrast, consider these subtypes of extrinsic motivation, which fall along the continuum of internalization (Ryan and Deci 2000, Deci and Ryan 1985, 2002). The more an individual has internalized an external regulation (e.g. ISP), the more autonomous she/he will perceive the compliance with this regulation. According to SDT/OIT, an individual's perception of autonomy, competence, and relatedness will increase an individual's motivation to perform a particular behavior with enhanced performance, persistence, and creativity. OIT particularly focuses on an individual's psychological need for autonomy when performing a behavior, and considers human actions not as a consequence of expected incentives (exogenous motivation), but rather by the subjective psychological meaning of these stimuli (endogenous motivation).

This study employs the organismic perspective to augment our understanding regarding the impact of employees' endogenous motivation on their intention to comply with ISPs. Thereby the proposed model addresses a gap in the literature regarding the role of internalization, i.e. the integration of organizational security standards and values into one's own sense of self (Layton 2005, Siponen and Oinas-Kukkonen 2007). It is expected that the extent to which employees comprehend and internalize security policies and values influences their motivation to comply with ISPs. This survey develops and empirically validates a research model that integrates SDT/OIT with the theory of

planned behavior (TPB) (Ajzen 1991), and the concept of information security awareness (ISA). According to Vallerand's (1997) hierarchical model of motivation, the TPB and OIT/SDT provide complementary explanations: While the TPB is appropriate to explain specific target behaviors, SDT/OIT constructs represent individuals' general motivations in a specific context. Although the TPB and SDT/OIT are each well studied on their own, this study is the first to integrate them in the context of ISS research. Combining both theories with the concept of ISA provides valuable insights on how perceived self-determination and internalization of security policies affect the process that transforms employees' cognitive state of ISA into ISS-related behaviors.

The remainder of the study is organized as follows. First, a background overview of prior research on ISS behavior is given. Then the hypotheses are developed and the proposed research model is presented. After describing the research methodology, the results of the statistical analyses are outlined. Finally, the results are discussed, theoretical and practical implications are provided, the study's limitations and recommendations for future research are disclosed.

2 Background

Organizations' ISPs are often found to remain ineffectual to some extent as employees intentionally or unknowingly disobey security policies and standards (Foltz 2000, Besnard and Arief 2004, Lee et al. 2004). The literature argues that the observed limited effectiveness of ISPs is largely due to employees' lack of awareness of the respective ISPs (Thomson and von Solms 1998, Siponen 2000). Consequently, the concept of ISA has recently received increasing attention both by practitioners and scholars. and is considered as "one of the most important antecedents of behavior" (Siponen 2000). To increase employees' level of ISA and to encourage ISS behavior, organizations have introduced a broad variety of security education training and awareness (SETA) programs (e.g., Thomson and von Solms 1998, Peltier 2005, Puhakainen 2006, Rotvold and Braathen 2008, Puhakainen and Siponen 2010, Karjalainen and Siponen 2011). However, despite all of the efforts of management to raise ISA and to avoid harmful ISS behavior, there is still no guarantee that IS-users are motivated to act the way they are taught in SETA programs, or as desired or prescribed in the ISPs (Besnard and Arief 2004, Guo et al. 2011).

When it comes to explaining employees' motivation to comply with ISPs, the general deterrence theory (GDT) has been the dominating theoretical perspective (Siponen and Vance 2010). Originating in the field of criminal science, GDT contends that ISP compliance is largely driven by threats of sanctions for ISP violations, and the IS end-users' perceived certainty and severity of those sanctions. Building upon the GDT, D'Arcy and Hovav (2007a) and D'Arcy et al., (2009) show that employees' awareness of security countermeasures, such as ISPs, SETA programs, and monitoring activities positively influence the perceived severity and certainty of organizational sanctions associated with IS misuse, and therefore indirectly tend to reduce IS misuse intentions. D'Arcy et al. (2009, p. 80) contend that "from a deterrence perspective, security policies rely on the same underlying mechanism as societal laws: providing knowledge of what constitutes unacceptable conduct increases the perceived threat of punishment for illicit behavior". However, the effectiveness of deterrence mechanisms has often been questioned, since a variety of studies report inconclusive results (D'Arcy and Herath 2011). Hu et al. (2011) and Pahnila et al. (2007a) did not find any evidence that the

threat of sanctions significantly affected employees' ISP compliance. Similarly, Guo et al. (2011) found no evidence that employees' perceptions about the certainty of sanctions prevent ISP violations. Also, implementing deterrence security mechanisms, such as computer monitoring and sanctioning for ISP violations did not reduce the quantity and severity of ISS breaches (Wiant 2003). With regard to other extrinsic motivations, such as avoiding shame, informal penalties, or rewards the literature reports moderate or non-significant effects on individual ISP compliance (Pahnila et al. 2007b, Siponen and Vance 2010, Liang et al. 2013). Some scholars have even suggested that extrinsic motivations may negatively affect security behavior (Benabou and Tirole 2003). In his conceptual paper, Siponen (2000) suggests considering personality traits, such as morals, ethics, emotions, wellbeing and a feeling of security as important factors influencing individual motivations to act in accordance with organizational security guidelines. In a similar direction, further studies indicate that intrinsic and affirmative mechanisms ensuring commitment and participation, such as the perceived mental pleasure of committing the intended act (Hu et al. 2011), employees' perceived effectiveness of security behavior (Herath and Rao 2009a), organizational commitment (Herath and Rao 2009b), perceived legitimacy (Son and Rhee 2011), perceived intrinsic benefits (Bulgurcu et al. 2010), or the perceived fairness of the requirements of the ISPs (Bulgurcu et al 2009) positively affect employees' ISP compliant behavior.

These studies provide important insights into the role of extrinsic and intrinsic motivations, however, to my best knowledge no study exists that delves deeper into the role of endogenous motivations on ISP compliant behavior. Recent research on the SDT and OIT (Ryan and Deci 2000, Deci and Ryan 1985, 2002) in IS research (e.g., Malhotra et al. 2008, Wunderlich et al. 2013) and other domains, such as marketing (e.g., Cadwallader et al. 2010) and health behavior (e.g, Hagger and Chatzisarantis 2009) suggest that an individual's perceived autonomy in initiating a behavior directly impacts the likelihood that this behavior is actually performed. In particular, these studies found that if externally prescribed rules are congruent with individual values (internalization), following those rules is perceived as autonomously driven, which in turn leads to a higher likelihood of individuals to comply. External stimuli (e.g., ISPs) than have similar effects as intrinsic motivations. This is the difference between OIT and mechanistic motivational studies, which solely differentiate between extrinsic and intrinsic

motivation. Thereby OIT particularly focuses on the antecedents and impacts of different forms of extrinsic motivation, including external regulation, as measured by the construct external PLOC (low internalization) and identification and integration, as measured by internal PLOC (high internalization). External and internal PLOC are the end points of the internalization continuum. The more an extrinsic motivation is internalized, the more autonomous an individual will perceive his/her behavior. Therefore, OIT is particularly suited to understanding how extrinsic motivations regarding IS security influence the internalization of goals and norms included in organizational ISPs which can lead to resistance, partial compliance, or full internalization of IS security goals. Against this background, and in line with the calls of Siponen (2000), Layton (2005) and Siponen and Oinas-Kukkonen (2007) to discover ISP compliance motivations by means of intrinsic motivation, TPB, and ISA, this study derives a model, which integrates all three concepts.

3 Theoretical Framework and Hypotheses

3.1 Theory of Planned Behavior

The TPB (Ajzen 1991) has been proven to be a compelling social cognitive framework to explain situation specific influences on intentional behaviors across a variety of disciplines. TPB claims that human behavior is essentially rational and largely relies on an individual's intention. Intention can be interpreted as the extent of willingness and effort that an individual plans to invest in performing a behavior (Ajzen 1991). Although intention does not replace actual behavior, as a strong motivational determinant it accounts for a respectable amount of variance in the actual behavior (Ajzen 1991). Hence, if intentions are high, the corresponding behavior is likely to occur. According to the TPB, the prediction of intention relies on three belief-based variables: Attitude towards the behavior, normative beliefs, and perceived behavioral control (Ajzen 1991). Consistent with the literature, I used self-efficacy instead of perceived behavioral control "...because the latter essentially measures the same latent construct as self-efficacy (Fishbein 2007) and originates from self-efficacy theory (Bandura 1977)" (Bulgurcu et al. 2010, p. 528).

3.1.1 Attitude

Attitude is defined as the degree to which an individual regards a behavior in question or its outcomes as favorable or unfavorable (Fishbein and Ajzen 1975). Accordingly, in the context of this study, attitude represents the degree to which an employee thinks it is favorable or unfavorable to comply with ISPs. This is largely dependent on beliefs about the consequences of compliance and how positively evaluated these consequences are (Bulgurcu et al. 2010). Prior research in various fields, such as the adoption of IT (e.g., Jan and Contreras 2011, Al-Ajam and Nor 2013), environmental friendly behavior (e.g., Greaves et al. 2013), use of Green-IS (e.g., Kranz and Picot 2011, Wunderlich et al. 2013) or engaging in health-preserving behaviors (e.g., Hagger et al. 2006, Protogerou et al. 2013) has shown that attitude towards a behavior is a reliable predictor of intention. Furthermore, studies in the ISS field provide ample support for the positive impact of attitude on ISS intentions (e.g., NG and Rahim 2005, Dinev and Hu 2007, Pahnila et al. 2007a, Bulgurcu et al. 2009 and 2010, Anderson and Agarwal 2010). Based on broad

empirical evidence that attitude is a strong predictor of behavioral intention, the following hypothesis is proposed:

Hypothesis 1: Attitude towards ISP compliance positively influences an individual's intention to comply with the ISP.

3.1.2 Self-Efficacy

Bandura's self-efficacy theory suggests that an individual evaluates his abilities and resources to fulfill certain tasks, spearing that one's task-specific level of self-confidence determines the behavioral outcomes (Yiu et al. 2012). Transferred to the field of ISS, self-efficacy is defined as "… an employee's judgment of personal skills, knowledge or competency about fulfilling the requirements of the ISP." (Bulgurcu et al. 2010, p. 529). Earlier research across a wide variety of behaviors has proven that employees are more motivated and make more effort with tasks for which they have high levels of self-efficacy (Yiu et al. 2012). In addition, in ISS research there exists considerable evidence on the crucial role of self-efficacy in shaping information security behavior. Woon et al. (2005) found self-efficacy to be a significant predictor of using security features on home wireless networks. Rhee et al (2009) showed that IS end-users with higher self-efficacy in ISS significantly use security protection software more often, demonstrate more security conscious care behavior, and exert more effort to strengthen information security. Others found self-efficacy and perceived behavioral control to foster IS end-users' intention to use anti-spyware technologies (e.g., Dinev and Hu 2007, Johnston and Warkentin 2010). Investigating antecedents of ISP compliance, Pahnila et al. (2007b), Herath and Rao (2009b), Siponen et al. (2009, 2010) and Bulgurcu et al. (2010) also found that self-efficacy, referring to whether employees believe that they can apply and adhere to ISPs, has a significant effect on their intention to comply with ISPs. Hence,

Hypothesis 2: Self-efficacy to comply with ISP positively influences an individual's intention to comply with the ISP.

3.1.3 Normative Beliefs

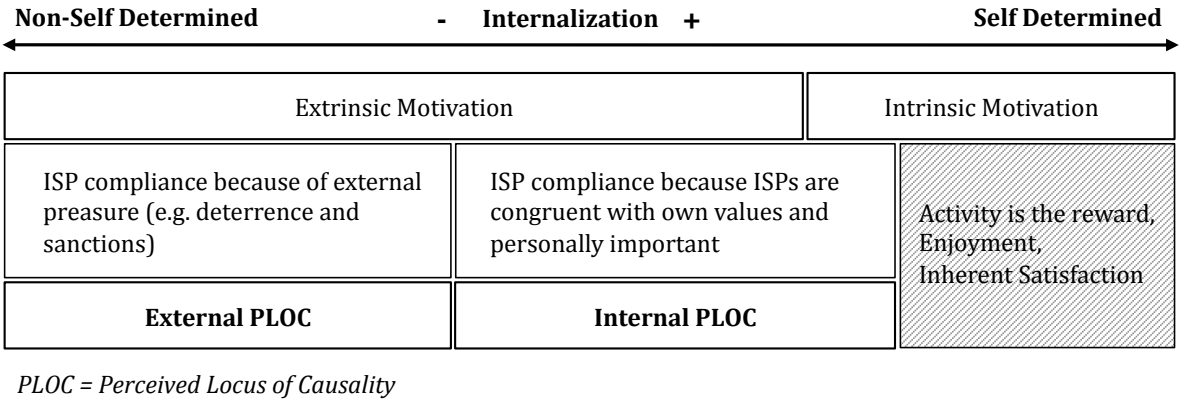
A broad range of research across the fields of social psychology (Fulk et al. 1987, Manning 2011), general behavioral science (Childers and Rao 1992, Fischbein and Ajzen 1975), and technology adoption (Wunderlich et al 2013) has shown that people's behavior is influenced by normative beliefs and social influences. In the context of this study, normative beliefs are defined as "… an employee's perceived social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers." (Ajzen 1991, Bulgurcu et al. 2010, p. 529). The positive influence of normative beliefs on IS-users' intentions to comply with ISPs has been shown by several ISS studies (e.g. Pahnila 2007a and 2007b, Herath and Rao 2009a, Siponen et al. 2009, Bulgurcu et al. 2010). In line with previous research, the following hypothesis is stated:

Hypothesis 3: Normative beliefs about ISP compliance positively influence an individual's intention to comply with the ISP.

3.2 Self-Determination Theory / Organismic Integration Theory

Hitherto, the ISS literature predominantly understood motivation from a mechanistic perspective, differentiating solely between extrinsic or intrinsic motivations. This perspective considers motivation to differ only in terms of amount (e.g. Bandura 1996), meaning that more motivated individuals "… will aspire to greater achievement and be more successful in their efforts than people with less motivation." (Cadwallader et al. 2010, p. 221). In contrast, OIT which is a sub-theory of SDT contends that the quality of motivation – exogenous vs. endogenous – is more important than the mere amount of motivation (Deci and Ryan 2002, Ryan and Deci 2000). This means that from an organismic perspective the same external stimuli (e.g., prescribed rules within ISPs) may motivate different behavioral responses depending on one's endogenous psychological feelings of autonomy or pressure with regard to the stimuli. OIT conceives behavior as either autonomously motivated, such that people perceive the behavior as initiated by choice of the self or controlled when a behavior is perceived as externally enforced (Deci et al. 1991).

To analyze an individual's perceived degree of autonomy, the OIT distinguishes between internal and external perceived locus of causality (PLOC) (Ryan and Connell 1989) (see Figure 15). The PLOC taxonomy is based on the theory of internalization which describes "... a continuum in which a social value or regulation is adopted as one's own or identified with." (Ryan and Connell 1989, p. 750). Internalization of external regulations results in these regulations being fully endorsed by the self (Deci et al. 1991). Hence, the more an external regulation is appropriated and internalized, the higher is the perceived level of autonomy in complying with this regulation (Ryan and Connell 1989). This contrasts OIT from SDT, which solely considers different degrees of perceived autonomy but does not build on the process of internalizing external regulations. Obeying rules under the influence of internal PLOC is thus caused by endogenous motivations that result from an individual's appraisal of the behavior in question as being personally meaningful, and therefore relate to intrinsic motivation, although the stimuli (e.g. ISP) seems to be of an extrinsic nature (Malhotra et al. 2008). In contrast, external PLOC refers to extrinsic motivation in its purest form, in that individuals who are motivated through external PLOC perceive their behavior as being controlled by external forces (Ryan and Connell 1989).



PLOC = Perceived Locus of Causality

Figure 15: Endogenous Motivation (Ryan and Connell 1989, Ryan and Deci 2000)

3.3 Integration of the Theory of Planned Behavior and Self-Determination Theory / Organismic Integration Theory

Both the TPB and SDT/OIT aim to explain human behavior. However, they differ in their level of generality (Vallerand 1997). While the TPB refers to a particular behavior, SDT/OIT relates to an individual's general motivations in a given context (Deci and Ryan 1985, Ryan and Connell 1989). Hence, PLOC influences behavior not only through "… the here and now of motivation …" (Vallerand 1997, p. 293), but beyond that is suggested to affect various behaviors in particular contexts, through more generalized motivations (Cadwallader et al. 2010, Wunderlich et al. 2013). In this regard, a connection can be drawn to Vallerand's (1997, 2000) hierarchical model of motivation, which suggests that due to the different degree of generality of contextual and situational motivations, the first affects the latter in a top-down fashion (Hagger et al. 2006, Wunderlich et al 2013).

Internal PLOC results from a high level of internalization of external regulations (Ryan and Connell 1989). If employees internalize the rules prescribed in the ISP, they adopt the regulation as their own and identify themselves with it because it is perceived as personally important and congruent with their own values (Ryan and Connell 1989). Thus, if an employee internalizes external regulations such as guidelines specified in ISPs, the likelihood of ISP-compliant behavior increases, since it is perceived as autonomous and personally relevant (Deci and Ryan 1985, Malhotra et al. 2008). The literature suggests that individuals who perceive themselves as the origin of their behavior will make great efforts and sacrifices to perform the behavior (Ryan and Deci 2000, Deci and Ryan 2002, Turban et al. 2007). Hence, it is suggested:

Hypothesis 4: Internal PLOC positively influences an individual's intention to comply with the ISP.

According to the TPB, the attitude towards a behavior is defined as an individual's evaluation of performing a specific future behavior as desirable (positive) or undesirable (negative) (Fishbein and Ajzen 1975, Malhotra et al. 2008). Prior research in other domains found that a high level of internal PLOC positively influences the attitude towards the respective behavior (Hagger et al. 2006, Wunderlich et al. 2013). It

is expected that employees, having internalized the security guidelines, perceive compliance to be necessary and beneficial for them and their organization. Hence,

Hypothesis 5: Internal PLOC positively influences an individual's attitude towards ISP compliance.

Self-efficacy describes an individual's evaluation of their own abilities and resources with respect to a specific behavior (Bandura 1977). Individuals who have internalized external regulations (e.g., prescribed rules) usually aim at finding out how to fulfill those regulations (Ryan and Connell 1989). Turban et al. (2007) investigated the effects of PLOC in the context of work task performance and found that individuals with high levels of internal PLOC use their cognitive capabilities more intensively, and that they are motivated to acquire the required know-how to perform the expected task. This should lead to higher levels of self-efficacy. Accordingly, for this study it is expected that employees whose own values display a high level of congruence with the rules prescribed in the ISP strive more thoroughly to acquire the competences needed to avoid unintentional misbehavior. Thus,

Hypothesis 6: Internal PLOC positively influences an individual's self-efficacy to comply with the ISP.

External PLOC refers to the least autonomous form of extrinsic motivation. Accordingly, behavior motivated through external PLOC is a result of an individual's attainment (e.g., rewards) or avoidance of negative consequences (e.g., sanctions) administered by others (Deci and Ryan 1985). This kind of motivation does not rely on self-endorsement, but on motives attributed to external authority or compliance (Ryan and Connell, 1989). GDT claims that the perceived certainty and severity of sanctions for policy violations increases employees' compliance behavior. These deterrence mechanisms pertain to the external PLOC. Although deterrence mechanisms limit one's autonomy, they should still have a positive impact on ISP compliance as extrinsic motives, e.g., avoiding sanctions, and therefore may still be important for employees. However, under the influence of external PLOC, external regulations are not internalized, so that it is assumed that the effect of external PLOC on intention to comply will be weaker than that of internal PLOC (Ryan and Connell 1989, Dholakia 2006, Malhotra et al. 2008). Hence,

Hypothesis 7: External PLOC positively influences an individual's intention to comply with the ISP, however to a weaker extent than internal PLOC.

Even though individuals perceive their behavior as externally regulated, they could still value the outcome of the behavior, such as avoiding penalties for ISS related misconduct or being esteemed by colleagues and superiors (Deci and Ryan 1985). Accordingly, even though employees may perceive their security-related behavior as non-autonomous and externally regulated, they may still appreciate the personal or organizational benefits and usefulness of ISP compliance. Therefore, although employees might consider complying with ISPs as forced, they do it because they can profit from it. However, the effects are expected to be weaker than for internal PLOC, since attitude formation is influenced by extrinsic motivators (Ryan and Connell 1989, Malhotra et al. 2008).

Hypothesis 8: External PLOC positively influences an individual's attitude towards ISP compliance, however to a weaker extent than internal PLOC.

3.4 Information Security Awareness

Due to the socially constructed nature of ISA, there exists no one universal definition (Tsohou et al. 2008). In this study, ISA is defined as "an employee's general knowledge about information security and his cognizance of the ISP of his organization" (Bulgurcu et al. 2010, p. 532). This definition agrees with Siponen, who defined ISA as "… a state where users in an organization are aware - ideally committed to - their security mission (often expressed in end-user security guidelines)" (Siponen 2000, p. 31). Bulgurcu et al. (2010) differentiate between two ISA dimensions, general information security awareness (GISA) and information security policy awareness (ISPA). GISA corresponds to an individual's overall knowledge and understanding of ISS issues and their potential consequences, while ISPA refers to the knowledge and understanding of the requirements of the organization's ISP.

ISA is well known to be an essential determinant of an individual's ISS behavior. Galvez and Guzman (2009, p.4) identified ISA as one of the shaping factors of behavior and state that "… the higher the information security awareness, the higher the information security practice.". Dinev and Hu (2007) found that users' awareness of potential risks and threats of harmful ISS technologies determines the intention to make use of

protective information technologies. Bulgurcu et al. (2010) found significant positive effects of ISA on the three outcome beliefs (1) perceived benefit of compliance, (2) perceived cost of compliance and (3) perceived cost of noncompliance, as well as on attitude and intention to comply. Moreover they found that ISA's influence on an individual's intention to comply is partially mediated by attitude. I argue that employees with higher levels of ISA will assess ISP compliant behavior as more important than employees with lower levels of ISA, since they are more aware of the potential negative consequences that could result from ISP violations. Following the literature, it is suggested that ISA directly influences attitudes towards ISP compliance and that attitude partially mediates the positive effects of ISA on intention to comply. Hence,

Hypothesis 9a: ISA positively influences an individual's attitude towards ISP compliance.

Hypothesis 9b: The positive effect from ISA on intentions to comply will be partially mediated by attitude.

Although there exists sound support for the role of the different PLOC types for behavior, little research has concentrated on antecedents and individual factors determining the PLOC continuum (Turban et al. 2007). Turban et al. (2007) postulate a set of personality-related factors, such as extraversion, emotional stability and conscientiousness, which enhance the process of internalization of external regulations, and thus positively influence the internal PLOC. This raises the question, whether other factors on an individual level similarly influence an individual's level of PLOC. In a meta-analytical study concerning the PLOC continuum in the contexts of sport, exercise, and physical education, Chatzisarantis et al. (2003) found that an individual's perceived competence positively affected his/her level of internal PLOC. Due to ISA's knowledge dimension, ISA is closely related to an individual's perceived level of general competence regarding ISS. Hence, if users are well aware of the ISP requirements, they will be more likely to feel competent at performing compliance. The resulting behavior will then be motivated by internal PLOC, as the individual rather regards himself as the source of regulation. Siponen (2000) states that an employee's internalization of ISS regulations does not arise from itself, but is built on the gradual and long-term process

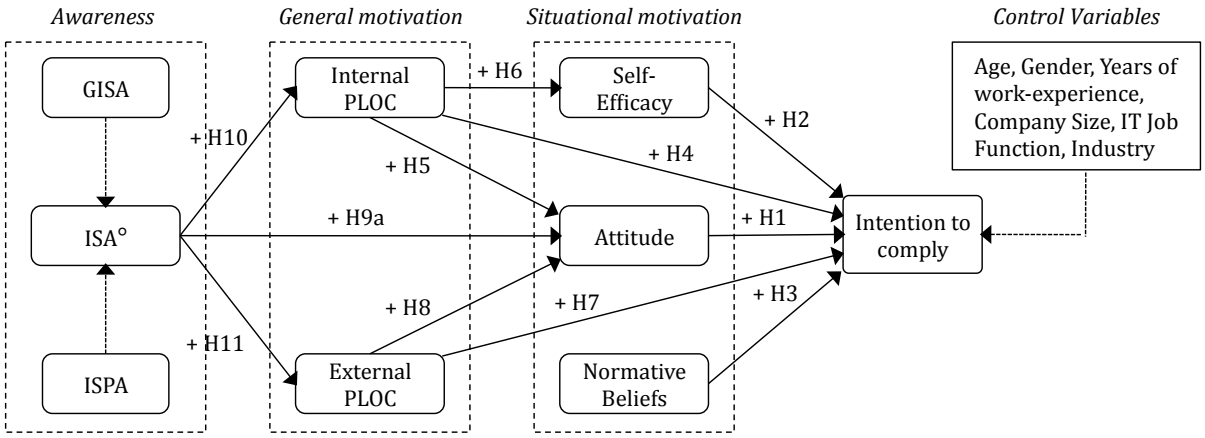
of raising the awareness of the regulations and of ISS in general. Against this background, it is assumed that high levels of ISA positively affect the internalization of ISPs. Thus,

Hypothesis 10: ISA is positively associated with an individual's level of internal PLOC.

On the other hand, it is supposed that ISA also precedes an individual's level of external PLOC. As an individual develops ISA he/she becomes aware of and learns about related consequences, such as rewards or punishments for compliance or non-compliance. This is consistent with the GDT perspective, which argues that high levels of ISA positively influence ISP compliant intentions through the increase of an individual's perception of the certainty and severity of sanctions (D'Arcy et al. 2009). Since behavior motivated through external pressure (e.g., threats of sanctions) is related to motivation via external PLOC, it is hypothesized that high levels of ISA increases individuals' levels of external PLOC.

Hypothesis 11: ISA positively influences an individual's level of external PLOC.

3.5 Proposed Research Model



° Second-order construct*; ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; PLOC = Perceived Locus of Causality*

Figure 16: Proposed Research Model

4 Research Methodology

In order to test the proposed research model and the underlying hypotheses, a quantitative survey method and structural equation modeling based on the component-based partial least square (PLS) approach are applied. In the following section, the details of the measurement instrument, the process of data gathering, and the sample of the study are illustrated.

4.1 Measures

To develop the survey instrument standard psychometric scale development procedures were conducted. The extant literature was carefully reviewed and empirically validated scales were adopted. The approach of applying pre-tested and empirically validated constructs was chosen, since it is known to provide the best reliability scores of the results (Straub 1989). All latent variables were measured reflectively with multiple items on seven-point Likert-scales with different poles, as described in Table 20. The dependent variable intention to comply, as well as the constructs of the TPB were adopted from Bulgurcu et al. (2010), who adapted Ajzen's constructs in the context of ISP compliance. For the operationalization of the two SDT/OIT constructs internal PLOC and external PLOC, the originally developed measures by Ryan and Connell (1989) were adapted to the context of ISP compliance. ISA was measured as second order construct following the definition and operationalization of Bulgurcu et al. (2010). Since all measures originated from English studies, the instrument was first developed in English and subsequently translated into German. In order to provide consistency in the meaning of the translated items, cross-translations with native speakers of both languages were conducted, with the consequence of minor adjustments in the wording of the items. In a second step, qualitative and quantitative pilot studies were conducted to validate the items for the scales, including sorting procedures with subsequent interviews of four practitioners and six scholars (Moore and Benbasat 1991). The pretests allowed for the checking and elimination of any instances of incomprehensibility, ambiguity or confusion within the items, as well as of the general mechanics of the questionnaire (e.g. survey instructions and completion time), and ensured initial reliability of the scales. After some minor

adjustments, the final survey instrument consisted of a set of 29 clear and understandable items and distinguishable constructs. A summary of all items along with their sources and factor loadings is illustrated in Table 20.

Following the suggestions of prior ISS research, extraneous control variables were included that potentially may influence ISS security behavioral aspects. The recipients were asked for demographic characteristics, such as age, gender, working experience, and whether or not they work in an IT function. Additionally, it was controlled for company size and four industry types that are known to be most critical and vulnerable to ISS incidents, namely “financial services”, “consulting”, “manufacturing”, and “information technologies and telecommunication”.

Construct (Source)	Items	Scale	Factor Loading
General Information Security Awareness (Bulgurcu et al. 2010)	Overall, I am aware of the potential security threats and their negative consequences.	a	.899***
	I have sufficient knowledge about the cost of potential security problems.	a	.782***
	I understand the concerns regarding information security and the risks they pose in general.	a	.822***
Information Security Policy Awareness (Bulgurcu et al. 2010)	I know the rules and regulations prescribed by the ISP of my organization.	a	.936***
	I understand the rules and regulations prescribed by the ISP of my organization.	a	.904***
	I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.	a	.930***
Internal Perceived Locus of Causality (Ryan and Connell 1989)	I comply with the requirements of the ISP…		
	(1) …because I want to ensure the ISS of my employer.	a	.863***
	(2) …because I think ISS is important.	a	.817***
	(3) …because I want to find out how to ensure ISS.	a	† .614***
	(4) …because I think it is important to comply with the ISP.	a	.824***
	(5) …because I would not want to violate the ISP.	a	.757***
External Perceived Locus of Causality (Ryan and Connell 1989)	I comply with the requirements of the ISP…		
	(1) …because I will get in trouble if I do not.	a	.799***
	(2) …because that is what I am supposed to do.	a	.803***
	(3) …so that my boss does not penalize me.	a	.697***
	(4) … because that is the rule.	a	.852***
	(5) … so others will not be angry with me.	a	† .514***
Attitude towards ISP compliance (Ajzen 1991; Bulgurcu et al. 2010)	To me, complying with the requirements of the ISP is _____.		
	unnecessary…necessary	b	.847***
	unbeneficial…beneficial	b	.696***
	unimportant…important	b	.858***
	useless…useful	b	.841***
Self-Efficacy to comply (Ajzen 1991; Bulgurcu et al. 2010)	I have the necessary _____ to fulfill the requirements of the ISP.		
	skills	c	.946***
	knowledge	c	.907***
	competencies	c	.934***
Normative Beliefs (Ajzen 1991; Bulgurcu et al. 2010)	_____ think that I should comply with the requirements of the ISP.		
	My colleagues	a	.849***
	My executives	a	.931***
	My managers	a	.800***
Intention to comply (Ajzen 1991; Bulgurcu et al. 2010)	I intend to comply with the requirements of the ISP of my organization in the future.	a	.969***
	I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	a	.945***
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	a	.960***

*** P < .001; † removed items; Scale a: Seven-point Likert scale: (1) "strongly disagree" –(7) "strongly agree"; scale b: Seven-point Likert scale: (1) = Extremely; (2) = Quite; (3) = Slightly; (4) = Neither; (5) = Slightly; (6) = Quite; (7) = Extremely; scale c: Seven-point Likert scale: (1) = Almost Never; (2) = Very Rarely; (3) = Rarely; (4) = Occasionally; (5) = Frequently; (6) = Very Frequently; (7) = Almost Always

Table 20: Measurement Items and Item Loadings

4.2 Data Sample

To test the model a large scaled online survey was conducted. Subjects were recruited by e-mail and links posted using multiple distribution channels, such as on- and offline business networks, business portals, and university alumni associations. Web-logs indicated that from 980 initial visitors, 578 finished the survey completely. After questions about the employee's demographics, the structure of the questionnaire proceeded with two exclusion criteria (Bulgurcu et al. 2010). First, unemployed and self-employed recipients were excluded, which resulted in a total of 55 exclusions. Second, the employees were asked whether their company has an explicitly formulated ISP. The implementation of this criterion lead to a further 53 exclusions of recipients whose employer had not constituted an ISP. Third, with the average response time for a completed questionnaire being 455 seconds, 18 questionnaires were excluded which showed a noticeably short response time ($t < 250$ seconds). Finally, a rough examination of the plausibility of several response schemes resulted in an elimination of a further 8 cases. The final sample consisted of $n = 444$ complete questionnaires. In order to examine the data for a possible non-response bias, the method recommended by Armstrong and Overton (1977) was adopted. As no significant difference between the first and the last third of the data was identified, a non-response bias could be ruled out.

The final sample population is composed of 32.0% female participants and has an average age of 35.3 years, ranging from 20 to 67 years. The distribution within the population regarding the type of industry results in 26.3% from the IT and telecommunication industry, 9.4% from manufacturing industry, 8.1% in consulting, 5.8% in financial services and 50.2% working in other industries. 16.2% of the participants stated that they work in an IT function. The working experience of the employees ranges from 0 to 46 years with a population average of 10.6 years. Finally, the company size is quite evenly distributed, with employees working for small, medium-sized and large organizations. Summarizing these findings, the data shows a diverse distributed sample population, with employees of a broad range of organizations, industries and personal backgrounds, and is therefore adequate for the following analysis. A detailed illustration of the sample demographics is summarized in Table 21.

Total Sample	**n = 444**	**100%**
Gender		
Male	307	69.1%
Female	137	30.9%
Age		
Min	20	
Max	67	
Mean	35.34	
20-25	40	9.0%
26-35	232	52.3%
36-45	106	23.8%
46-55	54	12.1%
56-65	10	2.2%
66 and over	2	0.4%
Industry		
Consulting	36	8.1%
Financial Services	26	5.8%
IT and Telecommunication	117	26.3%
Manufacturing	42	9.4%
Others	223	50.2%
IT Job Function	73	16.4%
Work Experience		
Min	0	
Max	46	
Mean	10.63	
< 2 years	65	14.6%
3-5 years	124	27.9%
6-10 years	86	19.3%
11-15 years	64	14.4%
16-20 years	34	7.6%
> 20 years	71	15.9%
Company Size		
less than 100 employees	81	18.2%
100-499	103	23.1%
500-999	29	6.5%
1.000-2.499	40	9.0%
2.500-9.999	66	14.8%
more than 9.999	125	28.1%

Table 21: Demographics of Participants

5 Analysis and Results

The research model was validated using structural equation modeling. In order to evaluate the psychometric measurement scales and to test the hypotheses, the component-based partial least square (PLS) approach using SmartPLS version 2.0.M3 (Ringle et al. 2005) was applied. As an alternative to covariance-based methods, the component-based PLS approach has received increasing attention in research, and is utilized in a variety of research fields, such as marketing, economics and behavioral science (Hair et al. 2012). Also in the field of ISS behavior research PLS has been the preferred choice in diverse, highly ranked IS-journals (e.g., D'Arcy et al. 2009, Bulgurcu et al. 2010, Siponen and Vance 2010). The PLS method was chosen because it is known for its ability to test complex latent-variable-based structural equation models with a minimum of methodological requirements, providing robust results (Johnson et al. 2006, Mayfield and Mayfield 2012). Following the two-step approach suggested by Anderson and Gerbing (1988), the psychometric properties of the measurement model were assessed first and subsequently the hypotheses were tested with the structural model.

5.1 Assessment of the Measurement Model

To evaluate the adequacy of the measurement model, the individual item and construct reliability, convergent validity and discriminant validity were analyzed (Gefen and Straub 2005).

In order to test the individual item reliability, which shows the extent to which an item is well suited to measure the corresponding construct, the factor loadings of all items on their respective latent variable were examined. As shown in Table 20, all items loaded significantly on their underlying latent variable, with values well above the recommended threshold of .707 (Chin 1998, Johnson et al. 2006) except for two items (internal PLOC_03 (.614) and external PLOC_03 (.514)), which were therefore eliminated from the measurement model. In order to verify the construct reliability (CR), composite reliability scores were assessed, which describe whether all items are consistently related to their corresponding latent variable (Mayfield and Mayfield 2012). In the literature, several threshold values are discussed, with Bagozzi and Yi (1994)

postulating a minimum value of .60, while other researchers propose a threshold of at least .70 (Nunnally 1978). As presented in Table 22, all CR values lay above both the thresholds. Further, the Cronbach alpha (CA) for each construct was calculated, which is based on the assumption that all items have the same relationship to the corresponding latent variable (Mayfield and Mayfield 2012). The CA proposed threshold of .70 is well exceeded by all latent variables (see Table 22). As a result, all scales show good reliability levels, since the criteria of indicator and construct reliability are met successfully.

In the next step, the convergent validity of the scales was assessed, by examining the constructs' average variance extracted (AVE) and the individual item reliability. As presented in Table 22, results show that the AVE score of each construct was well above the common threshold of .50 (Bhattacherjee and Premkumar 2004), and item reliability was given as examined before. Thus, convergent validity was satisfactory. The discriminant validity was evaluated applying the criterion of Fornell and Larcker (1981). All correlations between any two constructs were lower than the square root of the respective AVE. Additionally, a confirmatory factor analysis was conducted to check cross-loadings (see Appendix 11). All indicator items loaded significantly more on their corresponding construct than on any other construct (Gefen and Straub 2005). Accordingly, discriminant validity could be presumed. Summarizing the assessment of the measurement criteria, the measurement model appeared to be very adequate with regard to reliability and validity.

Variable	Range	Mean	SD	CR	CA	AVE	GISA	ISPA	IPLOC	EPLOC	ATT	SEE	NOB	INT
GISA	**1-7**	5.55	1.13	.874	.782	.698	**.836**							
ISPA	**1-7**	5.45	1.33	.946	.914	.853	.599	**.923**						
IPLOC	**1-7**	5.83	1.03	.894	.842	.679	.480	.492	**.824**					
EPLOC	**1-7**	4.51	1.41	.867	.807	.621	.102	.143	.320	**.788**				
ATT	**1-7**	5.72	1.09	.886	.830	.661	.455	.441	.622	.262	**.813**			
SEE	**1-7**	5.95	1.09	.950	.921	.864	.600	.586	.383	.052	.289	**.929**		
NOB	**1-7**	5.59	1.31	.896	.825	.742	.317	.402	.446	.332	.549	.310	**.862**	
INT	**1-7**	6.04	1.04	.971	.955	.918	.408	.526	.638	.249	.610	.346	.530	**.958**

SD = Standard Deviation; CR = Composite Reliability; AVE = Average Variance Extracted, CA = Cronbach Alpha; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; IPLOC = Internal Perceived Locus of Control; EPLOC = External Perceived Locus of Control, ATT = Attitude towards ISP compliance, SEE = Self-Efficacy to comply; NOB = Normative Beliefs, INT = Intention to comply; bold diagonal elements represent the square-root of AVE.

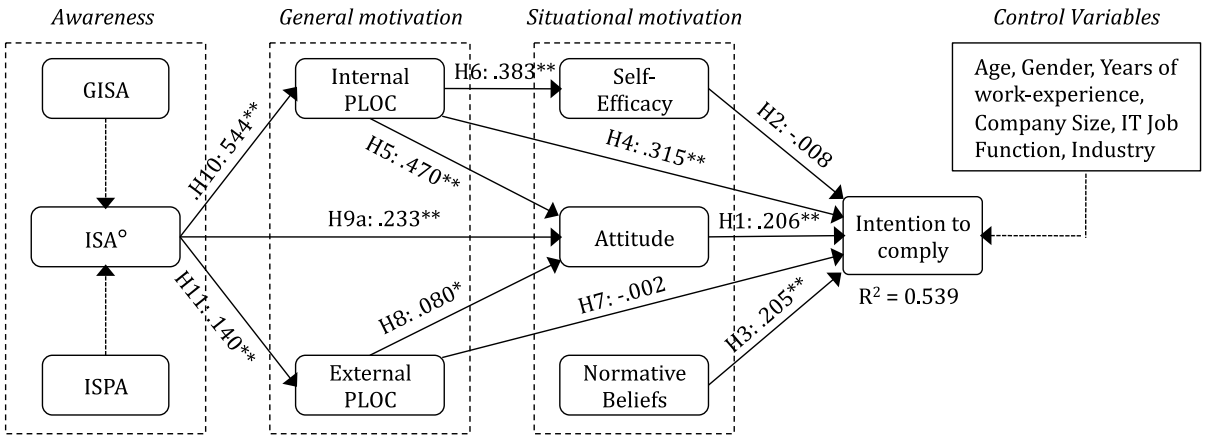
Table 22: Composite Reliability, AVE, and Latent Variable Correlations

5.2 Testing of the Structural Model

To validate the research model structural equation modeling was used. The significance of the parameter estimates was calculated using bootstrapping with 3,000 samples (Chin 1998). The model could explain a substantial portion of the variance in the dependent variable intention to comply (R^2 = .54). The removal of the control variables yield an R^2 of .53, implying that they only accounted for .01 of the variance in the intention to comply. None of the control variables were found to be significant (see Appendix 12). The weights of the two sub-dimensions GISA (w1 = .48) and ISPA (w2 = .64) of the second order construct ISA were significant ($p < .001$), indicating that each sub-dimension significantly contributed to the underlying overall factor (Bulgurcu et al. 2010). Since both independent and dependent variables were provided by the same respondents, it was tested for common method bias applying both the Harman's single-factor test (Podsakoff et al. 2003) and the marker variable test (Lindell and Whitney 2001). Both tests indicated that common method bias was not a threat to the validity of the study. To test the hypotheses, the respective path coefficients and their significance levels of the research model were tested as presented in Figure 17.

In accordance with hypothesis H1, an employee's attitude towards ISP compliance had a significant positive influence on the intention to comply with the ISP (β = .206, $p < .001$). Hence, hypothesis H1 was verified. In contrast to the expectations, self-efficacy to comply did not have a positive effect on intention to comply (β = -.008, n.s.). H2 needed to be rejected. Hypothesis H3 was supported, since normative beliefs were found to significantly impact on the intention to comply (β = .205, $p < .001$). In analyzing the interaction between the SDT/OIT and the TPB constructs, support for H4, H5 and H6 was found as the internal PLOC had strong and significant positive effects on the intention to comply (β = .315, $p < .001$), on attitude towards ISP compliance (β = .470, $p < .001$) as well as on self-efficacy to comply (β = .383, $p < .001$). A positive influence of the external PLOC on intention could not be proven (β = -.002, n.s.). Thus, hypothesis H7 was not supported. Hypothesis H8 could be verified, since external PLOC significantly preceded an individual's attitude (β = .080, $p < .05$). To test whether or not the effects of external PLOC on intention and on attitude are significantly weaker than the effects of internal PLOC on intentions and attitude, paired-sample t-tests were ran on the

bootstrapped path coefficients as suggested by Sarstedt and Wilczynski (2009). The results indicate that both the differences in the path coefficients from external PLOC and internal PLOC on intention as well as the differences in the path coefficients from external PLOC and internal PLOC on attitude are significant at a level of $p < .001$. Regarding the assumption that ISA positively influences attitude, strong support for hypothesis H9a ($\beta = .233$, $p < .001$) was found. ISA further showed a strong positive impact on internal PLOC ($\beta = .544$, $p < .001$) and a moderate impact on external PLOC ($\beta = .140$, $p < .01$), which results in the support of H10 and H11. Summarizing the testing of the structural model, all hypotheses were supported except for H2 and H7. An overview of the results of the structural analysis and hypotheses are illustrated in the following Figure 17 and in Appendix 12.



° Second-order construct; *ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; PLOC = Perceived Locus of Causality*

Figure 17: Results of Testing the Structural Model

5.3 Mediating Role of Attitude

To test the hypothesized mediating role of attitude, the widely used procedure proposed by Baron and Kenny (1986) was performed (see Figure 14 in Study II). The results of the mediation analysis are summarized in Table 23. To support significant mediation according to Baron and Kenny (1986) the following four conditions need to be fulfilled. First, the independent variable (ISA) must account for variations in the dependent variable (intention to comply), when not controlling for the mediator (attitude) (path c'). This condition was successfully met (ß = .235; $p < .001$). Second, the mediator must

significantly account for variations in the dependent variable (path b). This condition was likewise fulfilled (ß = .206, p < .001). Third, the independent variable must significantly account for variations in the mediator (path a). This condition was satisfied with (ß = .233; p <. 001). Finally, the effects of the independent variable on the dependent variables (path c') must decrease significantly when controlling for the mediator (path c). The results suggest the existence of a full mediation, if path c' becomes statistically insignificant when controlling for the mediator (path c), and suggests a partial mediation, if path c' only decreases but path c still stays significant.

Whether or not the mediation effect is significant can be examined by Sobel's (1982) test of indirect effects. It was tested whether the effects of the independent variable drops significantly once the mediator is incorporated into the model. The results in Table 24 show that the mediating role of attitude for the effects of ISA on the intention to comply was confirmed, as all four conditions were met. Furthermore, the Sobel's test revealed that the mediation effect was significant with p < .01. Since path c' decreases but path c still stays significant, attitude was found to partially mediate the effects of ISA on the intention to comply.

Hypothesis	**IV**	**Model II**			**Model I**	**Sobel's Test**	**Mediation**
		a	**b**	**c**	**c'**	z	
H9b	ISA	.233***	.206***	0.189***	0.235***	2.492**	Partial Mediation

ISA = Information Security Awareness; IV = Independent Variable; Model I: without controlling for the mediator (attitude); Model II: with controlling for the mediator; Path a: IV -> mediator; Path b: mediator -> intention; path c and c': IV-> intention; * p < .05; ** p < .01; *** p < .001.

Table 23: Mediation Analyses of Attitude

6 Discussion

The goal of this study was to develop and test a comprehensive model of employees' endogenous motivations to comply with organizational ISPs. Understanding which factors motivate ISP compliant behavior is crucial, as employees' compliant behavior has been found to be one of the most important determinants of successful ISS management (Ernst and Young 2005, Siponen and Vance 2010). Since prior research has neglected the important role of endogenous motivation and the internalization of ISPs, this study addresses this important gap in ISS literature and provides valuable insights both for practitioners and scholars. A model was developed and empirically tested that examines how TPB's situational constructs are influenced by contextual endogenous motivations represented by the SDT/OIT. Integrating the TPB, SDT/OIT and concept of ISA augments our understanding of the underlying motivational processes of ISP compliant behavior beyond the classical carrot and stick approach. The model was tested with survey data from 444 employees. In general, strong empirical support for the model was found, explaining a substantial proportion of the variance in ISP compliance intention (R^2 = .54).

6.1 Theoretical and Practical Implications

The TPB's constructs attitude towards ISP compliance, as well as normative beliefs, showed a significant positive effect on the intention to comply. These results underline the importance of an employee's perceived evaluation of ISP compliance as favorable or unfavorable, as well as the important role of the social environment and perceived expectations of others. Self-efficacy to comply was not found to significantly affect the intention to comply. This result may be sourced in the strong predictive power of the two constructs' attitude towards ISP compliance and internal PLOC, which may overlap the effects of self-efficacy.

The results provide strong empirical evidence that employees who perceive their behavior as self-determined and internalize ISS management's external regulations are more likely to comply with ISPs. In contrast, external PLOC had no impact on the intention to comply, implying that the effectiveness of traditional approaches based on deterrence or remuneration mechanisms are limited. Hence, employees who perceive

the regulations prescribed in the ISP as congruent with their own values have a significantly greater intention to comply with the ISP. The findings underscore the importance of establishing an organizational ISS aware culture (Haeussinger and Kranz 2013) that not only focuses on how employees should behave, but also why doing so is important for employees, the organization, and its customers and suppliers.

The combination of the TPB and the SDT/OIT confirms the hypothesis that general motivations at the contextual level (internal and external PLOC) strongly impact TPB's belief-based constructs at the situational level (Vallerand 1997, 2000), which significantly influence compliance intention. The integration of both theories particularly highlights the essential role of internal PLOC, since beyond its strong direct effect it also has an indirect effect on intention through attitude and self-efficacy. The relationship between external PLOC and attitude in contrast was only moderate, showing that employees' evaluations of the advantageousness of ISP compliant behavior are less dependent on external regulation than on personal motives and internalized values. The findings suggest that, while deterrence mechanisms surely remain important, they do not suffice to motivate employees' commitment to establishing ISS.

The findings strongly underscore the notion that ISA plays a pivotal role for ISP compliance (Siponen 2000a, Dinev and Hu 2007, D'Arcy et al. 2009, Bulgurcu et al. 2010) and show the different ways through which ISA affects compliance intentions. First, I found ISA to strongly determine an employee's level of internal PLOC. This shows that a certain level of ISA is required to catalyze the process of internalization. More specifically, and conforming with the notion of Siponen (2000), it implies that the process of internalizing ISS regulations does not arise from itself, but is built on a long-term foundation of general awareness and specific ISP knowledge. Second, ISA was also found to promote an employee's level of external PLOC. This finding indicates that ISA also forms an employee's perceived external pressure for ISP compliance, probably due to the higher awareness of the potential risks and consequences of non-compliance. Nevertheless, this effect seemed to be rather moderate. Last, but not least, ISA was found to positively influence the intention to comply directly and indirectly through an improvement of attitude towards ISP compliance. Moreover, attitude was found to partially mediate the positive effect of ISA on intention to comply. This confirms the

findings of Bulgurcu et al (2010), who similarly highlighted the key role of attitude in explaining the relationship between ISA and compliance intentions.

From a practitioner's point of view, the crucial challenge of aligning employees' ISS related behavior with a company's ISP requirements is to shift their perceived locus of causality from external to internal. Therefore, ISS practitioners should stimulate the internalization of security regulations. One step in this direction is to avoid presenting ISPs to employees without sufficiently explaining why these are critical for the company, and how even the smallest misconduct can have severe consequences. Further, security training should be designed to substantiate and explain the importance of security regulations, so that employees understand that their individual behavior can put them as well as their organization and customers at risk, to mitigate personal indifference. To avoid feelings of coercion, it should be made clear that ISPs do not exist to patronize employees, and that each rule has its goal. ISPs should also be aligned to the general interests of employees, such as having a secure job. The mediating role of attitude further suggests that security guidelines should appear desirable for employees. Techniques for achieving this aim are suggested by Siponen (2000). The importance of internal PLOC and the weak influence of external PLOC imply that deterrence-based mechanisms, like monitoring or punishment can only complement an effective security management. The results underscore the vital role of employees' security awareness on ISP compliant behavior. Hence, security managers must stay focused on ISA building/maintaining levers. In order to establish high ISA levels within the workforce, proper awareness programs and security training should be introduced aimed at enabling employees to understand the specifications and technological requirements connected to the ISP. Since there is no reason to believe that one awareness lesson will bring an employee to internalize and follow the ISP immediately, it is recommended to see the challenge of awareness raising as a gradual process and a long-term goal (Siponen 2000). Moreover, a comprehensive security aware culture should be developed within the organization to promote ISP compliance (Haeussinger and Kranz 2013).

6.2 Limitations

The study has some limitations that should be considered when interpreting the results. First, the data collection procedure was geographically confined to Western Europe. Hence, to generalize the findings, future research is needed to account for cultural differences, which may be of particular interest for multinational organizations. Second, the cross-sectional design of the data limits the generalizability of the findings in at least two ways: With regard to information security, user perceptions may change significantly over time, e.g. because of contemporary incidents. Also, the posited causal relationships can only be inferred. Thus, future research is encouraged to employ longitudinal research designs. Other limitations are due to restrictions of the measurement instrument.

Firstly in this connection, it had to rely on the intention to comply as the dependent variable instead of actual behavior. Although there exists empirical support that employees' intentions to comply with ISPs are significantly correlated with actual compliance behavior (e.g. Pahnila et al. 2007a), future research is needed to confirm the findings. Second, for the dependent variable "intention to comply", we used what Siponen and Vance (2014) call a generic measure. They argue that measurements of policy compliance intentions are more accurate if instrumentation includes contextualized examples of ISP compliance. Future research should address this limitation by applying more specific measures. Third, the applied operationalizations of IPLOC and EPLOC do not accurately reflect the PLOC continuum, but rather represent the end points of the continuum. Therefore, future research should use a relative measure of PLOC, e.g. following Hagger et al. (2006). Fourth, ISA was based on a perception-based measure, which is held as rather generic. Due to reasons of practicability and time restrictions, it could not be apply an extensive and differentiated list of questions for a more objective measure of ISA. Future studies could consider more complex measurement instruments to determine the construct of ISA.

6.3 Conclusion

A key goal of research on ISS is to identify and understand how managerially controllable antecedents influence employees' ISP compliance behavior. This study

provides important insights into the role of endogenous motivations guiding employees' intentions to comply with their organization's ISPs. By disentangling extrinsic and intrinsic motivations, my research provides new evidence on how ISP compliance is influenced by different endogenous psychological states, and reveals insights into why deterrence is not enough. By showing how ISA underpins motivational constructs of the TPB and the SDT/OIT, the study delves deeper into the notion that ISA is central to the formation of ISP compliant behavior. The study refines prior research, provides essential implications for practitioners and researcher, and serves as a starting point for further research into the role of users' endogenous motivations and values on ISS behavior. From a practitioner's point of view, the model can help to identify effective strategies to address and encourage employees to follow ISPs by increasing endogenous motivations and awareness of information security. Such strategies are expected to lead to a more persistent and superior behavioral performance (Deci and Ryan 2002).

F. General Conclusion and Implications

This dissertation set out to contribute to research in organizational information systems security (ISS) with a special focus on different aspects of employees' information security awareness (ISA) as part of the behavioral dimension of the domain. By building on prior theoretical considerations and empirical findings in the respective research field, this dissertation advances theory by reviewing and structuring the extensive literature on ISA, developing causal models and empirically testing derived hypotheses. The cumulative dissertation is comprised of three interrelated studies, each of which formulates a series of research questions.

The first paper is an extensive review of the existing body of knowledge of ISA research. The study identified and structured 131 selected ISA publications, which were then analyzed according to three main research questions, namely (1) "How is ISA conceptualized and defined in the literature?", (2) "How does ISA rely to information security behavior?", and (3) "Which factors influence ISA?". Thereby, the study follows the view that ISA does not equal ISS behavior or managerial awareness raising activities – a distinction which is often neglected by prior research. The study seeks to contribute to theory and practice by providing quick, structured access to the accumulated knowledge of ISA research, indicating the important implications for scholars and practitioners and revealing potential areas for further research. The literature review also served as a basis for the subsequent quantitative empirical papers 2 and 3, which focus on selected research gaps identified in paper 1.

Paper 2 and 3 are quantitative empirical examinations of specific, proposed research models that are directed at two distinctive essential facets of ISA research. The model in paper 2 addresses the lack of empirical studies exploring antecedents of employees' ISA by comprising specific institutional, individual, and environmental factors. Furthermore, the study examines the important, yet under examined, mediating role of ISA on the relationship between ISA's antecedents and employees' intention to comply with information security policies (ISPs). The model in paper 3 integrates the concept of ISA with general and situation specific motivational theories, in order to shed light on the complex question of how ISA and different types of endogenous motivation are linked together to explain the ISP compliant behavior of IS users. Data sets from two large

scaled online surveys were utilized, in order to test empirically the research questions posed. Thereby, both models synthesize various theoretical and socio-psychological perspectives, and represent a compromise between comprehensibility, parsimony, and generalizability. The results indicate ample support for the relationships hypothesized, and the explained proportions of the variance in the dependent variables were found to be substantial.

Each of the three studies provides extensive theoretical and methodical contributions, reveals implications for practice and policy makers, and points out potential avenues for future research. Since the dissertation is not without limitations, each study concludes by discussing these, as well as pointing out that they have to be taken into account in order to interpret the findings adequately. In the following section, the main findings and contributions of the three papers are briefly highlighted, selected recommendations for future research are underlined, and some concluding remarks are outlined.

Theoretical, Methodical and Practical Contributions

For a long time, research on ISS has concentrated predominantly on technological remedies, such as encryption, anti-spyware, virus detection, or firewalls. However, a more recent stream of literature shifts the focus to the behavioral dimension of ISS, since it is known that human error is directly or indirectly responsible for the majority of overall ISS incidents in organizations. With this in mind, to protect an organization's information assets against ISS threats and incidents most effectively, information security needs investments in both technical and socio-organizational resources (Bulgurcu et al. 2010). An essential artifact of the behavioral ISS domain is the exploration of several aspects around the topic of employees' ISA, which is acknowledged as one of the most influential determinants of ISS behavior. As mentioned before, this dissertation contributes to this stream of literature by providing an extensive literature review on the topic of ISA, advancing our understanding of which factors influence ISA, and which motivational processes transform ISA into ISP compliant behavior. The main theoretical and practical contributions, as well as selected recommendations for future research, are presented in the following by highlighting the distinct findings from each of the three papers.

The first study brought to light the fact that there is a lack of a stringent accordance within the literature's conceptualization of ISA. Moreover, the majority of studies do not even define the topic at all. Most frequently, the literature understands ISA as an individual's cognitive state of mind, which is characterized by recognizing the importance of information security and being aware and conscious about ISS objectives, risks and threats, and having an interest in acquiring the required knowledge to use IS responsibly. This dissertation follows this perspective of ISA. However, it is noticeable how frequently scholars use ISA and other very close objectives of ISS research, such as actual ISS behavior (e.g., ISP compliance) and managerial awareness raising methods synonymously. Hence, ISA is examined from multiple dimensions that cover "cognitive", "behavioral", and "procedural" aspects. Future research should address this vague and heterogeneous conceptualization of ISA in more depth by developing a generally accepted framework, which can then serve as a base for a coherent and clear assignment of the topic. The second focus of the literature review reveals that there are various studies applying multidisciplinary theories to explain individuals' information security behavior, but only a few studies which incorporate the concept of cognitive ISA. Since the literature emphasizes ISA to be one of the central antecedents of behavior, future empirical studies on ISS behavior are strongly recommended to take more thorough account of the effects of cognitive ISA. To explain the relationship between ISA and behavior, the general deterrence theory (GDT), the theory of planned behavior (TPB), and the technology acceptance model (TAM) were found to be the most dominant theories. In essence, and deviating from these theories, the literature highlights five key constructs through which ISA affects behavior indirectly, namely IS-users' perceptions of the severity and certainty that harmful ISS behavior will be sanctioned (GTD), attitude towards information security (TPB), and perceived usefulness and ease of use of information security technologies (TAM). Thus, from a deterrent perspective, security managers are suggested to monitor employees' behavior and to clearly communicate that harmful behavior and ISP violations will be detected and consequently sanctioned. From a technology acceptance perspective, practitioners are recommended to maximize the perceived ease of use of the respective information security countermeasures and to make their effectiveness as transparent as possible. The empirically supported and important mediating role of attitude implies that security managers should design SETA

programs in a way that reinforces employees' outcome beliefs and attitudes. Thereby shaping individuals' attitudes requires a gradual, long-term process. An appealing avenue for further research is to delve deeper into the question of how SETA programs should be designed to most effectively shape employees' attitudes towards ISP compliance in a sustainable way, since this is neglected by prior research. A further important key finding is that although deterrent mechanisms are known to play an important motivational role for ISP compliance, there are contradicting results, which indicate that future research should investigate individuals' compliance motivation from perspectives beyond coerced enforcement, such as self-determination and the consideration of personal values. There is also a lack of empirical studies exploring the potential moderating effects of different personal traits, such as morals and ethics, emotions, well-being, a feeling of security, rationality, and logic, as proposed by Siponen 2000a. The third focus of the study analyzed the literature on ISA according to the question of which factors precede individuals' ISA levels. Thereby, a broad set of institutional, individual, and environmental antecedents was identified. A major finding of this criterion of the literature review is the insight that although several antecedents of ISA are mentioned, there is a shortage of studies which provide empirical evidence for their hypotheses.

The second paper builds upon the first study and sets out to examine the basic question of which factors shape ISA, by developing and empirically testing a model that comprises six key antecedents of individual's cognitive ISA from institutional, individual, and environmental perspectives. The hypothesized positive effects of the antecedents examined (i.e. provision of security policies, SETA programs, employees' knowledge on IS, negative experience with ISS incidents, secondary sources' influence, and peer behavior) were all supported by the model and a substantial proportion of the variance in ISA was achieved. The model was validated using a sample of 475 employees from a diversified set of organizations. The major findings of the study include the points that the provision of security policies, and an employee's knowledge of information systems are the most influential antecedents of ISA. This indicates that managers should provide ISPs which are easily understandable and accessible on- and offline, at any time. This implication also conforms with international standards for best practice of information security management (ISM) ISO/IEC 27001 and 27002 (2005/2013) which stress the

importance of properly publishing and communicating an ISP document to all employees and relevant external parties in a form that is relevant, accessible and understandable. Furthermore, security managers should seek to improve the skills of those employees lacking general IS knowledge, so as to avoid accidental misbehavior. An interesting side outcome of the study is the found significant effect of the control variables working experience and gender. This indicates that female employees and employees with greater working experience have a significantly greater intention to comply with ISPs. The study also highlights the yet undiscovered mediating role of ISA between ISA's antecedents and behavioral intention, which is a valuable theoretical and methodological contribution to the behavioral ISS domain. Studies which investigate factors that influence ISS behavior should therefore account for the potential mediating effect of ISA. Another interesting finding is the good news that those antecedents of ISA which are controllable directly by information security managers (i.e., ISP provision, SETA programs, and IS knowledge) have a stronger impact on compliance intention through ISA than environmental variables (i.e., negative experiences, secondary source influence, peer behavior). However, differences in individual characteristics such as e.g., workload, overall job attitude, or organizational commitment could have an impact on the effectiveness of those institutional antecedents (Wipawayangkool 2009b). Future research is needed to address this issue empirically. Last but not least, it is important that scholars investigate and test further variables suggested to precede ISA, such as those identified in study 1 (e.g., personality traits (conscientiousness/agreeableness), organizational information security culture, managerial ISA, public ISA, individual education, and more specific forms of SETA programs).

The third study was guided by the basic question of why some employees are more motivated to comply with ISPs than others. The study's hypothesized relationships were analyzed in a sample of 444 employees from different organizations. The results contribute to present research on the relationship between ISA and behavior in several ways. The most intriguing finding was that high levels of congruence between employees' personal values and the rules and principles prescribed in ISPs (i.e. internal perceived locus of causality (IPLOC)) were found to play a major role in their motivation to comply, whereas the motivating effects of external pressure and coercion on the other hand (i.e. external perceived locus of causality (EPLOC)) were found to be limited. By

drawing on the role of endogenous motivation and the principle of self-determination, the results advance both theory and praxis, and contribute to the debate on the insufficient effectiveness of the predominant applied deterrence based approaches used to motivate employees' ISP compliance. From a practical point of view, the findings strongly suggest that security managers design ISPs in a way that employees are most likely to internalize them, and that a strategy which relies on pure extrinsic motivators, such as deterrence or remuneration mechanisms, is not sufficient. It is important that managers consider these requirements of ISPs already during the planning phase of their ISM system's development process, as prescribed by the international standards for best practice of ISM ISO/IEC 27001 and 27002 (2005/2013). The standards also give detailed advice for writing and implementing security policies most effectively. Another step in this direction is the establishment of SETA programs which do not only focus on how employees should behave, but also on emphasizing why even the smallest misconduct can have severe consequences for employees, the organization, its customers and suppliers. The findings of the study also acknowledge that employees' ISP compliance is driven by a blend of general contextual motivations (i.e. IPLOC and EPLOC)) and belief-based situation specific motivations (i.e. attitude and normative beliefs). Thereby the notion of Vallerand's (1997, 2000) hierarchical model of motivation, which suggests that, due to the different degree of generality of contextual and situational motivations, the former affects the latter in a top-down fashion could be confirmed. The results further brought to light that ISA precedes the different forms of endogenous motivations (i.e. IPLOC and EPLOC), as well as strongly affecting compliance intention both directly and indirectly via attitude. Hence the findings do not only confirm the notion that ISA plays a pivotal role for ISP compliance, but also provide new insights into the different ways through which this effect is achieved. A major management implication derived from these insights is that internalizing ISS regulations does not arise from it-self, but is built on a long-term foundation of general awareness and specific ISP knowledge. Security managers must stay focused on long-term ISA building and maintaining levers, and furthermore should emphasize a comprehensive security aware culture, in order to effectively and sustainably promote employees' ISP compliance.

Conclusion and Outlook

In conclusion, this dissertation set out to analyze different aspects of employees' information security awareness, which represents, more than ever, a fundamental artifact of modern information security management. The interest in private and corporate information security has developed considerably over the last few years, as have the advances in the young field of information security research. This development is not least driven by rapidly increasing global interconnectivity, innovations in information technologies, and the improvement of network infrastructures. In addition, the growing number of prominent information security breaches reflects this trend in which organizations suffer a loss of critical information, personal records, or other data, often resulting in serious financial damage and severe harm to their reputation. Both scholars and practitioners have come to realize that information security awareness is a fundamental factor for any successful information security management, as they acknowledge that information security is a multidimensional, rather than merely technical field, as traditionally supposed. Emerging from this shift in paradigms, researchers even suggest that investments in improving information security awareness are more cost effective than investments in advanced technologies (Jones 2007, Wipawayangkool 2009b). Recent accomplishments in information security research encourage this development, and security managers are more than ever interested in fostering employees' information security behavior through the use of policies, security trainings, and incentive systems. However, many questions concerning our understanding of the emergence of information security awareness and its closely related behavior remain unanswered. Future research is needed that builds upon the insights and limitations of this dissertation's studies, and validates their findings by employing different research designs, such as field experiments or experimental simulations. Furthermore, it is suggested that the empirical studies should be replicated in different settings, such as accounting for cultural differences, which may be of particular interest for multinational organizations. In summary, this thesis contributes to and subsequently advances research and practice in behavioral information security and discloses potential areas for prospective future research.

Appendix

Appendix 1: Correlation Between 131 Publications and Classification Scheme

Correlation Between 131 Publications and Classification Scheme (Criteria 1-5) (1 of 2)												
Author	**1**	**2**	**3**	**4**	**5**		**Author**	**1**	**2**	**3**	**4**	**5**
Albrechtsen (2007)	x		x	x	x		Furnell et al. (2002)				x	
Albrechtsen and Hovden(2010			x	x			Furnell et al. (2007)					x
Al-Hamandi (2006)	x				x		Galvez and Guzman (2009)	x	x			x
Al-Omari et al. (2011)	x	x		x	x		Goucher (2008)				x	
Al-Omari et al. (2012)	x	x		x	x		Greitzner et al. (2007)				x	
Aloul (2012)					x		Hagen and Albrechtsen (2009)				x	x
Banerjee and Pandey (2010)	x			x			Hansche (2001a)				x	x
Banerjee et al. (2013)	x			x	x		Hansche (2001b)				x	
Boujettif and Wang (2010)				x	x		Hawkins et al. (2000)					x
Bray (2002)	x						Heikka (2008)	x			x	x
Brez (2004)				x			Hellqvist et al (2013)	x				x
Bulgurcu et al. (2009)	x	x			x		Hentea (2005)				x	
Bulgurcu et al. (2010)	x	x	x		x		Herath and Rao (2009a)				x	
Calatayud (2011)	x			x			ISF (2007)	x			x	x
Casmir (2005)				x	x		ISO/IEC 27001 (2005, 2013)				x	x
Chan et al. (2005)				x			ISO/IEC 27002 (2005, 2013)				x	x
Chan and Wei (2009)				x			Jenkins et al. (2010)				x	
Chan and Mubarak (2012)	x				x		Jenkins et al. (2011)				x	
Charoen et al. (2007)			x	x			Johnson (2006)				x	
Chen et al. (2006)	x			x			Johnson and Koch (2006)					x
Choi et al. (2006)	x	x	x		x		Johnston and Warkentin (2010)				x	
Choi et al. (2008)	x	x	x		x		Kam and Katerattanakul (2014)				x	x
Cone et al. (2007)				x			Karjalainen and Siponen (2011)				x	
Cooper (2008)				x			Katsikas (2000)				x	
Cooper (2009)				x			Khan et al. (2011)	x			x	x
Cox et al. (2001)				x			Koskinen and Kelo (2009)				x	
CSI (2010/2011)					x		Kritzinger and Smith (2008)	x			x	x
Culnan et al. (2008)				x			Kruger et al. (2007)					x
D'Arcy and Hovav (2007a)	x	x		x			Kruger et al. (2010)		x			x
D'Arcy and Hovav (2007b)	x	x		x			Kruger and Kearney (2006)	x				x
D'Arcy and Hovav (2008)	x	x		x	x		Lebek et al. (2013a)		x			
D'Arcy et al. (2009)	x	x		x	x		Lebek et al. (2013b)					x
Desman (2003)				x			Lebek et al. (2014)		x			
Dinev and Hu (2007)	x	x			x		Lim et al. (2010)	x				
Dinev et al. (2009)	x	x			x		Mancha and Dietrich (2007)	x	x			
Dodge et al. (2007)				x	x		Mani et al. (2014)	x		x		x
Drevin et al. (2007)				x	x		McCoy and Fowler (2004)				x	
Eminağaoğlu et al. (2009)				x	x		McElroy and Weakland (2013)				x	x
ENISA (2006)	x			x	x		Mitnick (2003)				x	
Fung et al (2008)				x	x		NG and Kankanhalli (2008)	x			x	
Furman et al. (2012)					x		NIST (2003, 2006)	x			x	x
Furnell (2006)			x				North et al. (2006)					x

Correlation Between 131 Publications and Classification Scheme (Criteria 1-5) (2 of 2)												
Author	**1**	**2**	**3**	**4**	**5**		**Author**	**1**	**2**	**3**	**4**	**5**
North et al (2010)			x		x		Wipawayangkool (2009a)	x				
Offor and Tejay (2014)				x			Wipawayangkool (2009b)	x		x		
Okenyi and Owens (2007)	x		x	x			Yayla (2011)		x			
Olesegun and Ithinin (2013)				x								
Payne (2003)				x								
Peltier (2000)				x								
Peltier (2005)	x			x								
Power and Forte (2006)				x								
Puhakainen (2006)		x		x	x							
Puhakainen a. Siponen(2010)				x	x							
Qudaih et al. (2014)				x								
Rahim et al. (2008)				x	x							
Rantos et al. (2012)					x							
Rastogi and von Solm (2012)	x			x								
Rezgui and Marks (2008)	x		x		x							
Rotvold and Braathen (2008)	x		x	x								
Rotvold (2008)			x	x	x							
Rounds et al. (2008)					x							
Ryan (2007)			x		x							
Ryan (2006)		x	x		x							
Sari and Cadiwan (2014)					x							
Shaw et al. (2009)	x		x	x	x							
Siponen (2000)	x	x	x	x								
Siponen (2001)	x		x									
Sommers a. Robinson (2004)			x	x								
Spears and Barki (2010)	x	x	x		x							
Spurling (1995)	x		x	x								
Stanton et al. (2005)				x								
Steven and van Wyk (2006)				x								
Straub and Welke (1998)		x		x								
Takemura and Umino (2009)			x		x							
Takemura (2010)					x							
Takemura (2011)		x			x							
Talib et al. (2010)		x			x							
Thomson and v. Solms (1998)		x		x								
Thomson (1999)			x	x								
Tse et al. (2013)				x								
Tsohou et al. (2008)	x	x	x	x	x							
Tsohou et al. (2009)	x		x	x								
Tsohou et al. (2010)			x									
Vaast (2007)				x								
Valentin (2006)				x								
von Solms and v. Solms (2004)				x								
Waly (2012)				x								
Wilson and Hash (2003)				x								

1 = Definition of ISA; 2 = ISA's Relationship with Behavior; 3 = Antecedents of ISA; 4 = Security, Education, Training and Awareness (SETA) Programs; 5 = Assessment of ISA.

Appendix 2: Holistic Guidelines for SETA Program Management (Academical)

Holistic Guidelines for SETA Program Management (Academical)						
Author	**Key Issue / Finding**	**Emp. Evi.**	**Applied Theory**	**Method**	**Security Education, Training, Awareness**	**Target Group**
Banerjee et al. (2013)	Adapted the ISRA Model by Kritzinger and Smith (2008) to the software development process (audience group are software development teams), proposes an improvised software security awareness model entitled "ISSAM" which is an outcome of mapped and synchronized software development teams, software development life cycle phases with the various identified tools, techniques and methods of creating software security awareness.	N	-	Concept-ual	A	Soft-ware dev-elop-ment teams
Casmir (2005)	Deviates a dynamic and adaptive information security awareness (DAISA) approach, which delineates high-level guidelines for establishing and maintaining information security awareness programs at workplaces. The approach identifies 6-key elements of an effective SETA program. For the implementation the approach suggests an ISA program life cycle (evaluate, amend plan, plan and initiate, implement, evaluate.).	Y	Security learning continuum	Concept-ual and action research	SETA	All diff-erent target groups
Kritzinger and Smith (2008)	Develop an information security retrieval and awareness model (ISRA) for industry, which can be used by ISS managers to enhance information security awareness among employees.	N	-	Concept-ual	SETA	All diff-erent target groups

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = empirical evidence; N = no empirical study has been conducted.

Appendix 3: Holistic Guidelines and Standards of Good Practice for SETA Program Management (Practical)

Holistic Guidelines and Standards of Good Practice for SETA Program Management (Practical)						
Author	**Key Issue / Finding**	**Emp. Evi.**	**Applied Theory**	**Method**	**Security Education, Training, Awareness**	**Target-Group**
ENISA (2006)	Provides a holistic management guideline for planning and executing effective SETA programs.	N	-	Practical ex-perience	SETA	All different target groups
ISF (2007)	Suggests SETA management principles and objectives to raise awareness of information security enterprise-wide.	N	-	Practical ex-perience	SETA	All different target groups
ISO/IEC 27001 and 27002 (2005, 2013)	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	N	-	Practical ex-perience	SETA	All different target groups
NIST (2003, 2006)	Provides a holistic step-by-step management guide for executing the process (development, implementation, post-implementation) of effective ISA programs.	N	-	Practical ex-perience	SETA	All different target groups

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = empirical evidence; N = no empirical study has been conducted.

Appendix 4: Theoretical Frameworks for Designing Effective SETA Programs

Theoretical Frameworks for Designing Effective SETA Programs (1 of 2)						
Author	**Key Issue / Finding**	**Emp. Evi.**	**Applied Theory**	**Method**	**Security Education, Training, Awareness**	**Target-Group**
Drevin et al. (2007)	Identifies objectives for SETA programs by applying the value-focused thinking process which can serve as a basis for decision making and to guide the planning, shaping and development of SETA programs.	N	Value-focused thinking	Concept-ual	SETA	End-users
Heikka (2008)	Develop a theoretically grounded approach to IS security training based on constructivism. The approach is empirically validated in a telecommunications company and results show its positive impact on employees' security behavior.	Y	Construct-ivist learning theory	Case study, action research	Training	End-users
Karjalainen and Siponen (2011)	Develop a theoretical meta framework that posits four pedagogical requirements for designing effective ISS training approaches. Suggest "experiential learning cycle approach" by Kolb (1984) as one example approach that fulfills all four pedagogical requirements.	N	Meta-theory of three level thinking/ construct-ivism/ theory of experiential learning	Concept-ual	Training	All different target groups
Offor and Tejay (2014)	Suggest an effective SETA program to be based on adult-learner principles and should incorporate four training elements: motivation, reinforcement, retention, and transference.	N	Adult learner theory	Concept-ual	SETA	End-users
Puhakainen (2006)	Develops three novel design theories for improving IS-users' security behavior: (1) IS security awareness training, (2) IS security awareness campaigns, and (3) punishment and reward. These design theories aim to help practitioners to develop their own ISA approaches.	Y	Universal constructive instructional theory, elaboration likelihood model	Concept-ual, case study	SETA	All different target groups
Puhakainen and Siponen (2010)	Suggests that information security training should utilize contents and methods that activate and motivate the learners to systematic cognitive processing of information they receive during the training.	Y	Universal constructive instructional theory, elaboration likelihood model	Concept-ual, case study	SETA	All different target groups
Siponen (2000)	Provides a theoretical framework for persuasive approaches based on morals and ethics, wellbeing, a feeling of security, rationality, logic and emotions. Furthermore it stresses the need for normative approaches and motivational and behavioral theories as foundation for organizational SETA programs.	N	The theory of intrinsic motivation, TRA, TPB, TAM.	Concept-ual	SETA	End-users

Theoretical Frameworks for Designing Effective SETA Programs (2 of 2)						
Author	**Key Issue / Finding**	**Emp. Evi.**	**Applied Theory**	**Method**	**Security Education, Training, Awareness**	**Target-Group**
Straub and Welke (1998)	Considers SETA activities to be a form of organizations deterrent countermeasure as part of a security program, which aims to increase employees' knowledge of risks, policies, and sanctions in the organizational environment. A major aim of effective SETA programs is to convince potential abusers that the company will not treat intentional breaches of this security lightly.	Y	Deterrence theory	Qualitative field study	SETA	End-users
Thomson and von Solms (1998)	Utilize psychological principles to improve the effectiveness of SETA programs. They propose that ISS behavior can be changed in three ways: (1) directly changing their behavior, regardless of their attitude to the subject (2) using a change in behavior to influence a person's attitude, such as through role-playing exercises; and (3) changing a person's attitude through persuasion.	N	Social psychology principles	Conceptual	SETA	End-users
Thomson (1999)	Deviate guidelines and techniques for effective SETA programs based on social psychology principles. Some of the discussed techniques are instrumental learning, social learning, conformity, reciprocity, commitment, and self-persuasion (role-playing).	N	Social psychology principles	Conceptual	SETA	Management, It-Persona, end-users
Tsohou et al. (2009)	Linking SETA management activities (based on ENISA 2006, and NIST 2006) to the overall ISS management framework (plan, do, check, act) and identify interactions between their goals, roles, interdependencies or emergent events.	N	Management process plan, do, act, check	Conceptual	SETA	End-users

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = empirical evidence; N = no empirical study has been conducted.

Appendix 5: Causal Models Including Generic SETA Constructs

Causal Models Including Generic SETA Constructs						
Author	**Key Issue / Finding**	**Emp. evid.**	**Applied Theory**	**Method**	**Target-Group**	**Dep. Var.**
Al-Omari et al. (2011, 2012)	Awareness of SETA programs in general increase employees intention to comply indirectly via perceived usefulness of protection and perceived ease of use of protection.	Y	Technology Acceptance Model	Quantitative field study	End-users	Behavior
Chan et al. (2005)	Upper management practices (including SETA programs) enhance the organization's information security culture and ultimately employees' ISS behavior.	Y	-	Quantitative field study	End-users	Behavior
Culnan et al. (2008)	Employer sponsored corporate security awareness and training programs reduce home computer risks.	Y	-	Quantitative field study	End-users	-
D'Arcy and Hovav (2007a, 2007b, 2008), D'Arcy et al. (2009)	Show that the existence of SETA programs in organizations in general significantly decreases IS misuse behavior of employees through deterrent mechanisms.	Y	General deterrence theory	Quantitative field study	End-users	Behavior
Herath and Rao (2009a)	Show that management's resource availability including effective ISS trainings promotes an individual's level of perceived self-efficacy to comply with ISPs. Self-efficacy in turn was found to positively influence ISP compliance intentions.	Y	Protection motivation theory, GDT, TPB	Quantitative field study	End-users	Behavior
Jenkins et al. (2010)	Found that "users of corporate systems with more educational controls behave more securely than users of corporate systems with fewer educational controls" (password behavior)	Y	Dual-processing theory, expectancy value theory, yield shift theory	Experiment	End-users	Behavior
Mani et al. (2014)	Empirically emphasize that training employees on current security measures has a positive effect on information security awareness.	Y	Organizational Knowledge Creation Theory	Quantitative field study	End-users	ISA
Stanton et al. (2005)	Shows a significant correlation between the existence of SETA programs and password-related behaviors.	Y	-	Qualitative field study	End-users	Behavior
Wipawayangkool (2009b)	Within their causal model, they found that security training is positively associated with improvement in security awareness in 3 dimensions, namely cognition, affect, and skills.	Y	-	Quantitative field study	End-users	ISA / Behavior

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = empirical evidence; N = no empirical study has been conducted.

Appendix 6: Publications Investigating the Effectiveness of Specific SETA Methods

Publications Investigating the Effectiveness of Specific SETA Methods (1 of 3)							
Author	**Key Issue / Finding**	**SETA Method**	**Emp evid**	**Applied Theory**	**Method**	**Target Group**	**Dep. Var.**
Albrechtsen (2007)	Traditional SETA programs have little effect alone on user behavior and awareness. The users considers a user-involving approach to be much more effective for influencing user awareness and behavior.	User-participation	Y	-	Case study	End-users	ISA
Albrechtsen and Hovden (2010)	Involve employees in different workshops to talk and discuss their opinions on information security to subsequently develop an awareness program. Found that user participation enhances the participants' ISA and policy compliance behavior.	User-participation	Y	-	Intervention study	End-users	ISA and Behavior
Boujettif and Wang (2010)	Constructivist approach (user integration and learning autonomy) is more effective than classic SETA approaches. Applied the following user-integrated SETA methods: "email creation and antivirus", "videoed presentation", "quiz creation", "poster creation", "for and against discussion", "approximations", and "competition". One needs to consider that the constructivist approach also has disadvantages because it needs more time and resources.	User-participation	Y	Constructivist learning theory	Cases study	Software development teams	ISA and Behavior
Chan and Wei (2009)	Conduct an experiment and found that conceptual change fostered by anomalous data is effective in teaching information security awareness.		Y	Conceptual change	Case study, experiment	End-users	ISA
Charoen et al. (2007)	They developed and tested a training website for creating passwords to fit with theories pertaining to human memory. Participants of the study reported to obtain higher ISA and practice of using security passwords.	Web-based training for password security	Y	-	Action research, practical experience	End-users	ISA
Chen et al. (2006)	Develop an ISA system (ISAS) to manage and monitor all awareness raising activities within an organization. The main functions of the system include incident management, awareness activities management, and an evaluation management. The awareness activities are based on e-learning and covers news, discussion forums, mini-courses, broadcast messages, and online tests.	Web-based ISA management system	Y	System Development	Case study	End-users	ISA
Cone et al. (2007)	Preliminary results indicate that ISS online-games can be an effective addition to basic ISA training programs.	Online-game	Y	-	Case study	End-users	ISA

Publications Investigating the Effectiveness of Specific SETA Methods (2 of 3)							
Author	**Key Issue / Finding**	**SETA Method**	**Emp evid**	**Applied Theory**	**Method**	**Target Group**	**Dep. Var.**
Cox et al. (2001)	Examine three approaches to increasing awareness in an academic setting: a discussion session, a checklist and a web based tutorial. All three are found to be effective in raising motivation and understanding of security because they present the issues in an accessible, interesting way.	Discussion session / checklist / web based tutorial	Y	-	Action research, practical ex-perience	End-users	ISA
Dodge et al. (2007)	Conducted a fishingmail exercise primarly as assessment tool for ISA levels of employees but found it also to be an effective tool to raise ISA.	Fishing-mail exercise	Y	-	Experi-ment	End-users	ISA
Eminağaoğlu et al. (2009)	An ISA project with the focus on password usage, password quality and compliance of employees with password policies is implemented in a company over a period of 12 months both by training and awareness campaigns such as educational posters, animations and e-messages on the company Intranet, surveys and simple online quizzes.	SETA program with focus on password security	Y	-	Case study	End-users	ISA
Fung et al. (2008)	Suggests and test a simulation game called CyberCIEGE for raising ISA and knowledge of IS-users.	Online-game based training	Y	-	Experi-ment	End-users	ISA
Furnell et al. (2002)	Suggests a prototype security training software tool for information security awareness especially for small organizations with little resources.	E-learning software training tool	N	-	Practical experien ce	End-users	-
Greitzner et al. (2007)	Describe how to design an effective game-based training application in the domain of cyber security education	Online-game based training	Y	Cognitive and social learning theories	Experi-ment	End-users	ISA
Hagen and Albrechtsen (2009)	Measure and discuss the effects of an e-learning tool aiming at improving the ISA, and behavior of employees. Documents significant short-time improvements in ISA and behavior of participants.	E-learning tool	Y	-	Case study	End-users	ISA and Beha vior
Jenkins et al. (2011)	Suggest that security argumentation (e.g. training video) positively effects ISS behavior via an increase of attitude but also negatively affects it via higher cognitive load. Cues are suggested to have opposite effects.	Training video vs. cues	N	Cognitive Load Theory, elaborati on likelihoo d theory, TPB	Research in progress	End-users	Attit ude
Johnston and Warkentein (2010)	Show that messages that aim to persuade users to comply with policies through the arousal of fear impacted security behavior	Persuasive messages	Y	Fear appeal theory	Experi-ment	End-users	Beha vior

Publications Investigating the Effectiveness of Specific SETA Methods (3 of 3)							
Author	**Key Issue / Finding**	**SETA Method**	**Emp evid.**	**Applied Theory**	**Method**	**Target Group**	**Dep. Var.**
Kam and Katerattanakul (2014)	Showed that out-of-class learning is a viable pedagogical approach to support information security education through (1) first-year student retention and (2) first-year student motivation in learning.	Out-of-class learning	Y	College impact model	Experi-ment	End-users	-
Khan et al. (2011)	Discusses and evaluate the effectiveness of different information security awareness tools and techniques on the basis of psychological theories (TPB) and models. Found group discussions to be most effective.	Group discussion, posters, newslette, emails messaging, videogame	Y	TPB	Quantita tive field study	End-users	Beha vior
Koskinen and Kelo (2009)	Develop and test an e-learning course "Daily Information Security (DIS)" which consists of three components: active participation in online discussions, completion of practical assignments, and passing an oral examination.	E-learning Course	Y	-	Practical experien ce	End-users	Beha vior
NG and Kankanhalli (2008)	Investigate how different message characters (argument quality vs. quantity) based on persuasion principles and the elaboration likelihood model change a person's attitude.	Argument quality vs. quantity	Y	Info. process theory, per-suasion, ela-boration likely-hood	Experi-ment	End-users	Attit ude
Qudaih et al. (2014)	Discuss the use of persuasive technology principle to enhance ISA programs in organization.	Persuasive technology principles	N	-	Practical and theo-retical ex-perience	End-users	-
Rahim et al. (2008)	Tests the effectiveness of expert's presentations to change information security aware behavior and attitudes.	Expert's pre-sentation	Y	-	Inter-vention study	End-users	Beha vior and Attit ude
Rastogi and von Solm (2012)	Propose an information security service branding (ISSB) approach, which utilizes the concepts of brands and branding and operates by attempting to create a positive image of information security in the minds of end-users.	Infor-mation Security Service Brand (Process)	N	Service Branding Model	Con-ceptual	End-users	-
Shaw et al. (2009)	Conducts an experiment that investigates the impacts of hypermedia, multimedia and hypertext to increase information security awareness of end-users in an online training environment.	Media Richness of e-learning systems	Y	Cognitive load theory	Experi-ment	End-users	ISA
Sommers and Robinson (2004)	Suggest and test an effective approach in which students participate in developing their own awareness training video.	Training video with user part-icipation	Y	-	Action Research	End-users	ISA and Be-hav-ior

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = Yes; N = No.

Appendix 7: Advice for Contents, Methods, and Success Factors for Effective SETA Programs

Publications Discussing Contents, Methods, and Success Factors for Effective SETA Programs (1 of 3)					
Author	**Key Issue / Finding**	**Applied Theory**	**Method**	**Security Education Training, Awareness**	**Target-group**
Aloul (2012)	Discuss several key factors that are necessary to develop a successful information security awareness program.	-	Practical experience	Awareness	End-users
Banerjee and Pandey (2010)	Analyzes problems and prospects of promoting ISA of steakholders during software development processes.	-	Literature Review	SETA	Software deve-lopment teams
Brez (2004)	Provides advice for SETA programs in the healthcare context according to the HIPAA (Health Insurance Portability and Accountability Act Security Standard 164.312(a)(1)) and suggests to implement security reminders, log-in monitoring, password management, and protection of malicious software .	-	Practical experience	SETA	End-users
Cooper (2008)	Guideline for planning SETA programs (lessons learned)	-	Action research, practical experience	SETA	End-users
Cooper (2009)	Guideline for planning contents of SETA programs (lessons learned)	-	Action research, practical experience	SETA	End-users
Desman (2003)	Discuss "ten commandments of Information Security Awareness Training" and provide advice for planning or building SETA programs.	-	Practical experience	SETA	End-users
Goucher (2008)	Gives practical tips for raising awareness with security trainings.	-	Practical experience	SETA	End-users
Hansche (2001a, 2000b)	Discuss the process of designing and developing an ISA program and suggests success factors for developing and implementing awareness program /	-	Practical experience	Awareness	All different target groups
Hentea (2005)	Discusses issues to improve information security awareness education in public universities.	-	Practical and theoretical experience	Education	End-users
Johnson (2006)	Good practical essay which gives discuss issues to be considered when building SETA programs. Advice topics include "costs and benefits of a security program", "topics and target audiences", "measuring effectiveness", and "communication methods".	-	Practical experience	SETA	All different target groups
Katsikas (2000)	Discusses SETA program content for healthcare managers.	-	Practical experience	SETA	End-users

Publications Discussing Contents, Methods, and Success Factors for Effective SETA Programs (2 of 3)					
Author	**Key Issue / Finding**	**Applied Theory**	**Method**	**Security Education Training, Awareness**	**Target-group**
Mccoy and Fowler (2004)	Discuss the process of how they designed and developed an ISA program in an university setting and point out the stumbling blocks which they encountered along the way.	-	Practical experience	SETA	End-users
Mitnick (2003)	Discusses how organization can prevent from social engineering attacks.	-	Practical experience	SETA	End-users
Okenyi and Owens (2007)	Illustrate strategies for developing and implementing a successful ISA program to prevent human hacking attacks. Establish a security policy, identify current training needs, obtain management support, determine audiences, define key messages, define available Communication vehicles, develop a strategy for implementation, measure effectiveness.	-	Practical experience	Awareness	End-users
Olesegun and Ithinin (2013)	Explain how they created and implemented an information security awareness training (ISAT) program and discuss the impediment they encountered along the process. The program consists of training based on web, personal or individual training with a specific monthly topic, campus campaigns, guest speakers and direct presentations to specialized groups.	-	Practical experience	SETA	End-users
Payne (2003)	Discuss several key factors that are necessary to develop a successful information security awareness program including target audiences, delivery methods and communication tips.	-	Practical experience	SETA	End-users
Peltier (2000)	Suggests means to convey the awareness message: training sessions, books, videos, brochures, newsletters, booklets, and practice with the help of an instructor.	-	Practical experience	SETA	End-users
Peltier (2005)	Addresses the elements that make up a successful information security awareness program including goals, IS security training needs identification, program developments, methods for IS security training, and program presentations.	-	Practical experience	SETA	End-users
Power and Forte (2006)	Case study on the launch of a comprehensive awareness and education program for a global organization. Illustrate essential components of an effective SETA program, and explore some of the critical issues involved in developing it, rolling it out and institutionalizing it.	-	Practical experience	SETA	End-users
Rotvold and Braathen (2008)	Provides security awareness training guidelines for university students including topic lists and skills that can be applied to students' everyday lives and to their future careers in business.	-	Practical and theoretical experience	SETA	End-users

Publications Discussing Contents, Methods, and Success Factors for Effective SETA Programs (3 of 3)					
Author	**Key Issue / Finding**	**Applied Theory**	**Method**	**Security Education Training, Awareness**	**Target-group**
Rotvold (2008)	Provides security awareness training advice and highlights the importance to create a information security culture. Among others, management support and a proper foundation of SETA programs on policies is emphasized.	-	Practical experience	SETA	End-users
Spurling (1995)	Conducts a case study, which features an Australian company that experienced many user related information security problems which were resolved through a diverse set of strategies including newsletters, screen savers, books, and staff training.	-	Case study	SETA	End-users
Steven and van Wyk (2006)	Suggest that effective awareness and training programs should consider different audience groups. They emphasize 3 levels of training, e.g. executive level, management level, and special security groups, which will aid in behavior and environment transformation of people by means of education.	-	Practical and theoretical experience	SETA	End-users
Tse et al. (2013)	Discuss trends, questions, and possible solutions of information security issues in the banking industry. Results emphasize that banks should organize a formal SETA program including an ISA-system in e-learning platform that targets different level of staffs such as executives, professional and general staffs.	-	Case study	SETA	Manageme nt, It-Personal, end-users
Vaast (2007)	Analyzes social representations of ISS in the healthcare environment and draws strategic implications for research and practice. One major implication is that SETA programs should be customized to different target audiences.	-	Case study	SETA	End-users
Valentin (2006)	Suggests a multi-phased advice guideline, which incorporates three key components: assessment phase, identification phase, education phase.	-	Practical and theoretical experience	SETA	End-users
Steven and van Wyk (2006)	Gives practical recommendations about essential factors for successful security awareness training for software development teams. Suggests to run pilot trainings to identify audience needs, apply exercises, and use computer-based training (CBT) tools.	-	Practical and theoretical experience	Training	Software deve-lopment teams
von Solms and von Solms (2004)	Address the process of integrating policies, education and culture. They highlight the importance to properly communicate the policies via SETA programs to make them an effective tool of ISS management.	-	Conceptual	SETA	End-users
Waly et al. (2012)	Investigate and identify characteristics of effective training.	TPB, TRA	Qualitative field study	SETA	End-users
Wilson and Hash (2003)	A practical bulletin that provides guidelines and recommendations for designing, developing, and implementing a SETA program. The bulletin is a practical summary of NIST (2003, 2006).	-	Practical experience	SETA	End-users

Note. The tables in Appendix 2 – 7 are the result of a self-developed categorization of SETA literature; Y = empirical evidence; N = no empirical study has been conducted.

Appendix 8: Assessment of Information Security Awareness

Assessment of Information Security Awareness (1 of 3)									
Author	**Context ***	**P/S ****	**Goal *****	**Construct**	**Question-naire**	**Inter-view**	**Obser-vation**	**Experiment/ Testing**	**Audits**
Albrechtsen (2007)	O	P	A			x			
Al-Hamdani (2006)	P/U	P	B		x				
Al-Omari et al. (2012)	O	S	D	x	x				
Aloul (2012)	O/U	P	B		x	x	x	x	x
Banerjee et al. (2013)	O	S	B/C		x	x	x	x	
Boujettif and Wang (2010)	O	P	C		x	x			
Bulgurcu et al. (2009, 2010)	O	S	D	x	x				
Casmir (2005)	O	S	C		x		x		
Chan and Mubarak (2012)	U	P	A		x				
Chan and Wei (2009)	U	S	C		x			x	
Choi et al (2006, 2008)	O	S	D	x	x				
CSI (2010/2011)	O	S	C		x	x	x	x	x
D'Arcy and Hovav (2007a, 2007b, 2008), D'Arcy et al. (2009)	O	S	D	x	x				
Dinev and Hu (2007, 2009)	O	S	D	x	x				
Dodge et al. (2007)	U	P	C					x	
Drevin et al. (2007)	U	S	B			x			
Eminağaoğlu et al (2009)	O	S	C		x	x	x		
ENISA (2006)	O	S	B/C		x	x	x	x	x
Fakeh et al. (2012)	O/U	S	D	x	x				
Fung et al. (2010)	U	S	C		x				
Furman et al. (2012)	P	P	A		x	x			
Furnell et al. (2007)	P	P	A		x				
Galvez and Guzman (2006)	O	S	D	x	x				
Hagen and Albrechtsen (2009)	O	S	C	x	x				
Hansche (2001a)	O	S	C		x	x	x	x	

Assessment of Information Security Awareness (2 of 3)									
Author	**Context ***	**P/S ****	**Goal *****	**Construct**	**Questionnaire**	**Interview**	**Observation**	**Experiment/ Testing**	**Audits**
Hawkins et al. (2000)	O	P	A			x	x		
Heikka (2008)	O	S	C			x			
Hellqvist et al. (2013)	U	P	A		x	x			
ISF (2007)	O	S	C		x	x	x	x	x
ISO/IEC 27001 and 27002 (2005, 2013)	O	S	C		x	x	x	x	x
Kam and Katerattanakul (2014)	U	S	C		x	x			
Khan et al. (2011)	O	S	C		x		x		
Kritzinger and Smith (2004)	O	S	B/C		x				
Kruger et al. (2010)	U	P	B	x	x				
Kruger et al. (2007)	U	P	A					x	
Kruger and Kearney (2006)	O	P	C	x	x				
Lebek et al. (2013	O	P	B		x	x	x		
Mani et al. (2014)	O	S	D	x	x				
McElroy and Weakland (2013)	O	P	C		x	x	x	x	
NIST (2003, 2006)	O	S	B/C		x	x	x	x	
North et al. (2010)	U	P	A		x				
North et al. (2006)	U	P	A		x				
Puhakainen (2006), Puhakainen and Siponen (2010)	O	S	B/C		x	x			
Rahim et al. (2007)	O/U	P	C	x	x				
Rantos et al (2013)	O	P	C		x	x	x	x	
Rezgui and Marks (2008)	U		A		x	x	x		
Rounds et al. (2008)	U	P	A		x				
Rotvold (2008)	O	P	A		x				
Ryan (2006, 2007)	U	S	C		x				
Sari and Cadiwan (2014)	P	P	C		x				
Shaw et al. (2009)	U	S	C		x			x	
Spears and Barki (2010)	O	S	D	x	x				
Takemura and Umino (2009) Takemura (2010, 2011)	O/P	S	D	x	x				

Assessment of Information Security Awareness (3 of 3)									
Author	**Context ***	**P/S ****	**Goal *****	**Construct**	**Question-naire**	**Inter-view**	**Obser-vation**	**Experiment/ Testing**	**Audits**
Talib et al. (2010)	O/P	P	A	x	x				

Note. This table is the result of a self-developed categorization of the assessment methods of ISA.* O = Organization; P = Private; U = University. ** P = Assessment of ISA is main (primary) objective of the paper; S = Assessment of ISA is not main (secondary) objective of the Paper. *** A = Assessment of the general state of ISA; B = Assessment of the need for SETA programs; C = Assessment of the effectiveness of SETA programs; D = Causal models which incorporate an operationalization of ISA as construct.

Appendix 9: Crossloadings (Study II)

Item	INT	NEX	GISA	ISPA	ISPP	ISK	PEB	SETA	SSI
INT_1	**.969**	.089	.298	.233	.310	.267	.155	.287	.177
INT_2	**.947**	.077	.244	.278	.238	.329	.203	.322	.203
INT_3	**.961**	.056	.219	.249	.321	.301	.198	.211	.211
NEX_1	.038	**.871**	.025	.034	-.048	-.058	-.098	-.014	-.011
NEX_2	.027	**.796**	.025	.024	.011	-.063	-.072	-0.010	-.029
GISA_1	.283	.241	**.897**	.550	.384	.341	.233	.313	.251
GISA_2	.293	.043	**.772**	.464	.316	.369	.178	.372	.196
GISA_3	.236	.092	**.820**	.461	.354	.230	.268	.268	.258
ISPA_1	.221	-.005	.535	**.935**	.607	.283	.402	.499	.206
ISPA_2	.203	.074	.574	**.904**	.597	.322	.368	.419	.212
ISPA_3	.234	.028	.534	**.931**	.539	.281	.382	.470	.209
ISPP_1	.321	-.069	.249	.342	**.558**	.147	.314	.450	.163
ISPP_2	.278	-035	.416	.584	**.946**	.148	.495	.536	.248
ISPP_3	.340	-.012	.366	.585	**.907**	.152	.443	.565	.205
ISK_1	.343	-.040	.382	.282	.124	**.914**	-.031	.100	-.027
ISK_2	.289	-.070	.292	.292	.165	**.924**	.034	.113	-.051
ISK_3	.278	-.090	.362	.310	.154	**.929**	.044	.122	-.002
PEB_1	.178	-.102	.248	.399	.460	.001	**.951**	.432	.252
PEB_2	.135	-101	.261	.365	.468	-.009	**.918**	.454	.280
PEB_3	.167	-.085	.249	.390	.481	.054	**.909**	.453	.267
SETA_3	.290	.003	.361	.476	.562	.094	.440	**.951**	.245
SETA_4	.301	-.030	.302	.383	.467	.172	.449	**.776**	.207
SETA_5	.266	-.027	.346	.470	.532	.083	.416	**.928**	.262
SSI_1	.156	.034	.133	.131	.170	-.066	.187	.195	**.844**
SSI_2	.125	-.025	.283	.220	.235	-.024	.263	.262	**.958**
SSI_3	.139	-.045	.312	.243	.254	-.008	.313	.263	**.957**

INT = Intention to comply; ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; ISPP = Information Security Policy Provision; SETA = Security Education Training Awareness program; ISK = Information Systems Knowledge; NEX = Negative Experience; SSI = Secondary Sources' Influence; PEB = Peer Behavior.

Appendix 10: Results of Structural Model Analyses (Study II)

Hypothesis	Path	Path coefficient	T-values	Significance*	verified?
H1	ISA -> INT	.296	5.070	p < .001	yes
H2a	ISPP -> ISA	.398	9.034	p < .001	yes
H3a	SETA -> ISA	.148	3.091	p < .001	yes
H4a	ISK -> ISA	.307	7.725	p < .001	yes
H5	NEX-> ISA	.071	2.326	p < .001	yes
H6a	SSI -> ISA	.124	3.724	p < .001	yes
H7a	PEB -> ISA	.089	2.267	p < .05	yes
CV	AGE -> INT	.040	.920	n.s.	
CV	COSZ -> INT	.027	.950	n.s.	
CV	ITJO -> INT	-.014	.617	n.s.	
CV	WOEX -> INT	.094	1.762	p < .05	
CV	Gender -> INT	-.137	3.813	p < .001	
CV	Ind_M -> INT	.038	.837	n.s.	
CV	Ind_CS -> INT	.021	.298	n.s.	
CV	Ind_FS -> INT	-.079	.938	n.s.	
CV	Ind_IT -> INT	-.009	.209	n.s.	
CV	Ind_O -> INT	.012	.898	n.s.	
ISA Construct	GISA -> ISA	.466	37.269	p < .001	
ISA Construct	ISPA -> ISA	.650	34.940	p < .001	
R^2 of INT	.406				
R^2 of ISA	.501				

INT = Intention to comply; ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; ISPP = Information Security Policy Provision; SETA = Security Education Training Awareness program; ISK = Information Systems Knowledge; NEX = Negative Experience; SSI = Secondary Sources' Influence; PEB = Peer Behavior; CV = Control Variable; COSZ = Company Size; Ind_M = Industry_Manufacturing; Ind_CS = Industry_Consulting; Ind_FS = Industry_Financial Services; Ind_IT = Industry_IT and Telecommunication; Ind_O = Industry_Others; n.s. = not significant; * two tailed.

.

Appendix 11: Crossloadings (Study III)

Item	GISA	ISPA	IPLOC	EPLOC	ATT	NOB	SEE	INT
GISA_01	**.899**	.560	.433	.093	.399	.288	.529	.377
GISA_02	**.782**	.479	.312	.069	.348	.224	.489	.304
GISA_03	**.822**	.458	.454	.092	.394	.279	.484	.339
ISPA_01	.538	**.936**	.456	.159	.423	.385	.525	.503
ISPA_02	.583	**.904**	.441	.112	.391	.354	.559	.462
ISPA_03	.538	**.930**	.466	.124	.408	.375	.541	.493
IPLOC_01	.440	.464	**.879**	.230	.559	.443	.349	.576
IPLOC_02	.543	.479	**.844**	.117	.529	.364	.448	.495
IPLOC_04	.287	.351	**.820**	.313	.473	.305	.255	.519
IPLOC_05	.268	.297	**.747**	.448	.481	.347	.171	.515
EPLOC_01	.061	.105	.225	**.795**	.204	.302	.037	.184
EPLOC_02	.061	.090	.258	**.806**	.225	.258	.037	.198
EPLOC_03	.013	.064	.098	**.679**	.094	.211	.005	.077
EPLOC_04	.137	.160	.337	**.862**	.247	.270	.062	.258
ATT_01	.391	.393	.518	.215	**.847**	.464	.257	.527
ATT_02	.291	.268	.371	.202	**.696**	.395	.165	.372
ATT_03	.425	.409	.632	.240	**.860**	.476	.287	.613
ATT_04	.352	.339	.449	.192	**.840**	.443	.204	.422
NOB_01	.297	.324	.405	.283	.520	**.849**	.268	.483
NOB_02	.278	.375	.415	.317	.506	**.931**	.270	.484
NOB_03	.241	.343	.325	.253	.378	**.800**	.265	.394
SEE_01	.549	.521	.363	.030	.234	.272	**.946**	.310
SEE_02	.594	.594	.380	.084	.318	.300	**.907**	.338
SEE_03	.523	.513	.320	.027	.247	.291	**.934**	.312
INT_01	.392	.499	.615	.255	.610	.530	.324	**.969**
INT_02	.404	.513	.620	.228	.564	.478	.350	**.945**
INT_03	.377	.500	.598	.233	.579	.514	.320	**.960**

INT = Intention to comply; ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; ISPP = Information Security Policy Provision; SETA = Security Education Training Awareness program; ISK = Information Systems Knowledge; NEX = Negative Experience; SSI = Secondary Sources' Influence; PEB = Peer Behavior.

Appendix 12: Results of Structural Model Analyses (Study III)

Hypothesis	Path	Path coefficient	T-values	Significance*	verified?
H1	ATT -> INT	.206	2.968	p < .001	yes
H2	SEE -> INT	-.008	.150	n.s.	no
H3	NOB -> INT	.205	4.124	p < .001	yes
H4	IPLOC -> INT	.315	5.530	p < .001	yes
H5	IPLOC -> ATT	.470	8.897	p < .001	yes
H6	IPLOC -> SEE	.383	8.033	p < .001	yes
H7	EPLOC -> INT	-.002	.0450	n.s.	no
H8	EPLOC -> ATT	.080	2.246	p < .05	yes
H9a	ISA -> ATT	.233	4.606	p < .001	yes
H10	ISA -> IPLOC	.544	11.977	p < .001	yes
H11	ISA -> EPLOC	.140	2.807	p < .001	yes
CV	Age -> INT	.014	.248	n.s.	
CV	Gender -> INT	-.040	1.152	n.s.	
CV	WOEX -> INT	.006	.120	n.s.	
CV	ITJO -> INT	-0,02	.651	n.s.	
CV	COSZ -> INT	-.003	.083	n.s.	
CV	Ind_M -> INT	.003	.073	n.s.	
CV	Ind_CS -> INT	.015	.489	n.s.	
CV	Ind_FS -> INT	-.034	1.020	n.s.	
CV	Ind_IT -> INT	-.001	.339	n.s.	
CV	Ind_O -> INT	.042	1.12	n.s.	
ISA Construct	GISA -> ISA	.481	28.231	p < .001	
ISA Construct	ISPA -> ISA	.635	35.548	p < .001	
$R^2$of INT with CVs	.539				
$R^2$of INT without CVs	.532				

INT = Intention to comply; ATT = Attitude toward ISP compliance; SEE = Self-Efficacy to comply; NOB = Normative Beliefs; IPLOC = Internal Perceived Locus of Causality; EPLOC = External Perceived Locus of Causality; ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; CV = Control Variable; COSZ = Company Size; Ind_M = Industry_Manufacturing; Ind_CS = Industry_Consulting; Ind_FS = Industry_Financial Services; Ind_IT = Industry_IT and Telecommunication; Ind_O = Industry_Others; n.s. = not significant; * two tailed.

References

Abraham, S. (2011). Information Security Behavior: Factors And Research Directions. Proceedings of the 17th Americas Conference on Information Systems (AMCIS), USA, Michigan, Detroit, Paper 462.

Ajzen, I. (1985). From intentions to actions: A Theory of planned behavior, Action-control: From Cognition to Behavior. J. Kuhl and J. Beckmann, (eds), Heidelberg, Springer.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp. 179–211.

Al-Ajam, A. S., and Nor, K. M. (2013). Internet Banking Adoption: Integrating Technology Acceptance Model and Trust. *European Journal of Business and Management*, Vol. 5, No. 3, pp. 207–215.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, Vol. 26, No. 4, pp. 276–289.

Albrechtsen, E. and Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, Vol. 29, No. 4, pp. 432–445.

Al-Hamdani, W. A. (2006). Assessment of Need and Method of Delivery for Information Security Awareness Program. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (InfoSecCD), USA, Georgia, Kennesaw, pp. 102–108.

Al-Omari, A., El-Gayar, O., and Deokar, A. (2011). Information Security Policy Compliance: A User Acceptance Perspective. Proceedings of the 6th Annual Conference of the Midwest Association for Information Systems (MWAIS), USA, Nebraska, Omaha, Paper 12.

Al-Omari, A., El-Gayar, O., and Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective. Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS), USA, Hawaii, Honolulu pp. 3317–3326.

Aloul, F. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology (JAI*T), Vol. 3, No. 3, pp. 176 – 183.

Anderson, C. L., and Agarwal, R. (2010). Practicing Safe Computing: A multimethod empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly,* Vol. 34, No. 3, pp. 613–643.

Anderson, J. C., and Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin,* Vol. 103, No. 3, pp. 411–423.

Armstrong, S. J., and Overton, T. S. (1977). Estimating Non-Response Bias in Mail Surveys. *Journal of Marketing Research*, Vol. 14, No. 3, pp. 396–402.

Aytes, K. and Connolly, T. (2003). A Research Model for Investigating Human Behavior Related to Computer Security. Proceedings of the 9th Americas Conference on Information Systems (AMCIS), USA, Florida, Tampa, pp. 2027–2031.

Bagozzi, R. P. and Yi, Y. (1994), Advanced Topics in Structural Equation Models. Advanced Methods of Marketing Research, Cambridge, MA: Blackwell, pp. 1–5.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, Vol. 84, No. 2, pp. 191–215.

Bandura, A. (1989). Human Agency in Social Cognitive Theory. *American Psychologist,* Vol. 44, No. 9, pp. 1175–1184.

Bandura, A. (1996). Self-Efficacy: The Exercise of Control. New York, Freeman.

Banerjee, C., Banerjee, A., and Murarka, P. D. (2013). An Improvised Software Security Awareness Model. *International Journal of Information, Communication and Computing Technology*, Vol. 1, No. 2, pp. 43–48.

Banerjee, C., and Pandey, S. K. (2010). Research on software security awareness. *ACM SIGSOFT Software Engineering Notes*, Vol. 35, No. 5, pp. 1–5.

Baron, R. M., and Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology*, Vol. 51, No. 6, pp. 1173–1182.

Bassellier, G., Benbasat, I., and Reich, B.H. (2003). The Influence of Business Managers' IT Competence on Championing IT. *Information Systems Research,* Vol. 14, No. 4, pp. 317–36.

Benabou, R., and Tirole, J. (2003). Intrinsic and extrinsic motivation. *Review of Economic Studies,* Vol. 70., No. 3, pp. 489–520.

Besnard, D., and Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, Vol. 23, No. 3, pp. 253–264.

Bhattacherjee, A., and Premkumar, G. (2004). Understanding Changes in Belief and Attitude toward Information Technology Usage: A Theoretical Model and Longitudinal Test. *MIS Quarterly*, Vol. 28, No. 2, pp. 229–254.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A, and Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems,* Vol. 18, No. 2, pp. 151–164.

Boujettif, M., and Wang, Y. (2010). Constructivist Approach to Information Security Awareness in the Middle East. Proceedings of the 5th International Conference on

Broadband, Wireless Computing, Communication and Applications (BWCCA-2010), Japan, Fukuoka, pp. 192–199.

Bray, T. J. (2002). Security Actions During Reduction in Workforce Efforts: What To Do When Downsizing. *Information Systems Security*, Vol. 11, No. 1, pp. 11–15.

Bresz, F. P. (2004). People - Often the Weakest Link in Security, But One of the Best Places to Start. *Journal of Health Care Compliance*, Vol. 6, No. 4, pp. 57–60.

Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. Proceedings of the 17th European Conference on Information Systems (ECIS), Italy, Verona. Vol. 2009, pp. 2206–2217.

Brown, S., and Venkatesh, V. (2005). Model of Adoption of technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Quarterly*, Vol. 29, No. 3, pp. 399–426.

BS 7799-2 (2002). British Standard for Information Security Management. Part 2. Information Security Management Systems Specification with Guidance for Use, British Standards Institution (BSI), London, 2002.

BSI (2014). Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. URL: http://www.bsi.bund.de/gshb/.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. Proceedings of the 15th Americas Conference on Information Systems (AMCIS), USA, California, San Francisco, pp. Paper 419.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* Vol. 34, No. 3, pp. 523–527.

Brown, S. A., and Venkatesh, V. (2005). Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Quarterly,* Vol. 29, No. 3, pp. 399–426.

Cadwallader, S., Jarvis, C. B., Bitner, M. J. and Ostrom, A. L. (2010). Frontline Employee Motivation to Participate in Service Innovation Implementation. *Journal of the Academy of Marketing Science*, Vol. 38, No. 2, pp. 219–239.

Casmir, R. (2005). A Dynamic and Adaptive Information Security Awareness (DAISA) Approach. Doctoral Dissertation, Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology, Printed by Universitetsservice US-AB, Sweden, Stockholm.

Casmir, R. and Yngstrom, L. (2005). Towards a dynamic and adaptive information security awareness approach. Proceedings of the 4th World Conference on Information Security Education (WISE), IFIP TC11 WG11, Russia, Moscow.

Cavusoglu, H., Birendra, M., and Srinivasan, R. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, Vol. 9, No. 1, pp. 70–104.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. (2009). Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers. *Working paper,* Sauder School of Business, University of British Columbia.

Chan, K. (1998). Mass Communication and Pro-Environmental Behaviour: Waste Recycling in Hong Kong. *Journal of Environmental Management*, Vol. 52, No. 4, pp. 317–325.

Chan, H., and Mubarak, S. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications*, Vol. 60, No. 10, pp. 23–31.

Chan, Y. Y., and Wei, V. K. (2009). Teaching for conceptual change in security awareness: A Case Study in Higher Education. *Security & Privacy*, IEEE, Vol. 7, No. 1, pp. 68–71.

Chan M., Woon I., and Kankanhalli A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security,* Vol. 1, No. 3, pp. 18–41.

Charoen, D., Raman, M., and Olfman, L. (2007). Improving End User Behaviour in Password Utilization: An Action Research Initiative. *Systemic Practice and Action Research*, Vol. 21, No. 1, pp. 55–72.

Chatzisarantis, N. L., Hagger, M. S., Biddle, S. J., Smith, B., and Wang, J. C. (2003). A Meta-Analysis of Perceived Locus of Causality in Exercise, Sport, and Physical Education Contexts. *Journal of Sport and Exercise Psychology*, Vol. 25, No. 3, pp. 284–306.

Chen, H. , Chiang, R. H. L., and Storey, C., V. (2012a). Business intelligence and analytics: From big data to big impact. *MIS Quarterly,* Vol. 36, No. 4, pp. 1165–1188.

Chen, Y., Ramamurthy, K. and Wen, K. (2012b). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems,* Vol. 29, No. 3, pp. 157–188.

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

Cherdantseva, Y., and Hilton, J. (2013). A Reference Model of Information Assurance and Security. Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), IEEE, Germany, Regensburg, pp. 546–555.

Childers, T. L., and Rao, A. R. (1992). The Influence of Familial and Peer-Based Reference Groups on Consumer Decisions. *Journal of Consumer Research*, Vol. 19, No. 2, pp. 198–211.

Chin, W. W. (1998). The Partial Least Squares Approach for Structural Equation Modeling. *Modern Methods for Business Research,* G.A. Marcoulides (Hrsg.). Mahwah, NJ US, Lawrence Erlbaum Associates Publishers, pp. 295–336.

Chin, W. W., and Newsted, P. R. (1999). Structural Equation Modeling Analysis with small Samples using Partial Least Square Squares. *Hoyle, R. (Ed.): Statistical Methods for Small Sample Research,* Thousand Oaks, pp. 307–342.

Choi, N., Kim, D., and Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization' s Information Security Performance. Proceedings of the 12th Americas Conference on Information Systems (AMCIS), Mexico, Acapulco, pp. Paper 406.

Choi, N., Kim, D., Goo, J., and Whitmore, A. (2008). Knowing Is Doing: An Empirical Validation of the Relationship between Managerial Information Security Awareness and Action. *Information Management & Computer Security,* Vol. 16, No. 5, pp. 484–501.

Choi, S. Y., Lee, H., and Yoo, Y. (2010). The Impact of Information Technology and Transactive Memory Systems on Knowledge Sharing, Application, and Team Performance: A Field Study. *MIS Quarterly,* Vol. 34, No. 4, pp. 855–870.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. (2007). Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems*, Vol. 20, pp 958–971.

Cialdini, R. B., Reno, R. R., and Kallgren, C. A. (1990). A Focus Theory of Normative Conduct: Recycling the Concept of Norms to reduce littering in public places. *Journal of Personality and Social Psychology*, Vol. 58, No. 6, pp. 1015–1026.

Clinch J., (2009). ITIL v.3 and Information Security, Clinch Consulting, White Paper.

Compeau, D. R. and Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly,* Vol. 19, No. 2, pp. 189–211.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness*. Computers & Security*, Vol. 26, No. 1, pp. 63–72.

Cooper, M. (2008). Information security training: lessons learned along the trail, Proceedings of the 36th Annual ACM SIGUCCS Fall Conference on User Service, ACM, USA, Oregon, Portland, pp. 207–212.

Cooper, M. (2009). Information security training: what will you communicate?, Proceedings of the 37th Annual ACM SIGUCCS Fall Conference on User Service, ACM, USA, New York, New York, pp. 217–221.

Cox, A., Connolly, S., Currall, J., and Curall, J. (2001). Raising information security awareness in the academic setting. *Vine*, Vol. 31, No. 2, pp. 11–16.

Cronbach, L. J. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometirka,* Vol. 16, pp. 297–334.

Crossler, R. E. and Bélanger, F. (2006). The effect of computer self-efficacy on security training effectiveness. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (InfoSecCD), USA, New York, ACM Press, pp. 124–129.

CSI (2010/2011). The 15th Annual Computer Crime and Security Survey. Retrieved from: http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf

Culnan, M. J., Foxman, E. R., and Ray, A. W. (2008). Why IT Executives should help employees secure their home computers. *MIS Quarterly Executive*, Vol. 7, No. 1, pp. 49–56.

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

D'Arcy, J., and Hovav, A. (2007a). Towards a Best Fit between Organizational Security Countermeasures and Information Systems Misuse Behaviors. *Journal of Information System Security, Vol.* 3, No. 2, pp. 1–30.

D'Arcy, J., and Hovav, A. (2007b). Deterring Internal Information Systems Misuse. *Communications of the ACM,* Vol. 50, No. 10, pp. 113–117.

D'Arcy, J., and Hovav, A. (2008). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics*, Vol. 89, No. 1, pp. 59–71.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, Vol. 20, No. 1, pp. 79–98.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly,* Vol. 13, No. 3, pp. 319–340.

Deci, E. L., and Ryan, R. M. (1985). Intrinsic Motivation and Self-Determination in Human Behavior. New York, Springer US.

Deci, E. L., and Ryan, R. M. (2002). Handbook of Self-Determination Research. Rochester, University of Rochester Press.

Deci, E. L., Vallerand, R. J., Pelletier, L. G., Ryan, R. M. (1991). Motivation and Education: The Self-Determination Perspective. *Educational Psychologist*, Vol. 26, No. 3, pp. 325–346.

Desman, M. B. (2003). The Ten Commandments of Information Security Awareness Training. *Information Systems Security,* Vol. 11, No. 6, pp. 39–44.

Dholakia, U. M. (2006). How Customer Self-Determination Influences Relational Marketing Outcomes: Evidence from Longitudinal Field Studies. *Journal of Marketing Research*, Vol. 43, No. 1, pp. 109–120.

Diamantopoulos, A., Riefler, P., and Roth, K. P. (2008). Advancing Formative Measurement Models. *Journal of Business Research,* Vol. 61, No. 12, pp. 1203–1218.

Diamantopoulos, A., and Winklhofer, H. M. (2001). Index Construction with Formative Indicators: An Alternative to Scale Development. *Journal of Marketing Research*, Vol. 38, No. 2, pp. 269–277.

Dinev, T., and Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems,* Vol. 8, No. 7, pp. 386–408.

Dinev, T., Goo, J., Hu, Q., and Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, Vol. 19, No. 4, pp. 391–412.

Dodge, R. C., Carver, C., and Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, Vol. 26, No. 1, pp. 73–80.

Drevin, L., Kruger, H. A., and Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, Vol. 26, No. 1, pp. 36–43.

Elie-Dit-Cosaque, C., Pallud, J., and Kalika, M. (2011). The Influence of Individual, Contextual, and Social Factors on Perceived Behavioral Control of Information Technology: A Field Theory Approach. *Journal of Management Information Systems*, Vol. 28, No., pp. 201–234.

Eminağaoğlu, M., Uçar, E., and Eren, S. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, Vol. 14, No. 4, pp. 223–229.

ENISA (2006). A users' guide: How to raise information security aware- ness 2006. European Network and Information Security Agency. From http://www.enisa.europa.eu /doc/pdf/ deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf.

Ernst and Young (2003). Annual Global Information Security Survey. New York, USA.

Ernst and Young (2005). Annual Global Information Security Survey. Retrieved from: http://vistorm.com/uplds/EY_Global_Information_Security_survey_20051.pdf.

FIPS 200 (2013). Federal Information Processing Standards 200. Minimum Security Requirements for Federal Information and Information Systems. Carc.nist.gov. Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

Fishbein, M. (2007). A Reasoned Action Approach: Some Issues, Questions, and Clarifications. In Prediction and Change of Health Behavior: Applying the Reasoned

Action Approach, I. Ajzen, D. Albarracin, and R, Hornik (eds.), Hillsdale, NJ, Lawrence Erlbaum and Associates, pp. 281–296.

Fishbein, M., and Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. *Reading, MA, Addison-Wesley.*

Foltz, C. B. (2000). The impact of deterrent countermeasures upon individual intent to commit misuse: A behavioral approach. *Doctoral dissertation*, University of Arkansas, Fayetteville.

Fornell, C., and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research,* Vol. 18, No. 1, pp. 39–50.

Frank, J., Shamir, B., and Briggs, W. (1991). Security-Related Behavior of Pc Users in Organizations. *Information & Management*, Vol. 21, No. 3, pp. 127–135.

Fulk, J., Steinfield, J., and Power, G. (1987). A scoial information processing model of media in organizations. *Communication Research,* Vol. 14, No. 5, pp. 529–552.

Fung, C. C., Khera, V., Tantatsanawong, P., and Boonbrahm, P. (2008). Raising Information Security Awareness in Digital Ecosystem with Games – A Pilot Study in Thailand. Proceedings of the 2nd IEEE International Conference of Digital Ecosystems and Technologies (DEST), Thailand, Phitsanuloke, pp. 375–380.

Furman, S., Theofanos, M. F., Choong, Y.-Y., and Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *Security & Privacy*, IEEE, Vol. 10, No. 2, pp. 40–49.

Furnell, S. (2006). Remote Pc Security: Securing the Home Worker. *Network Security,* Vol. 11, pp 6–12.

Furnell, S. M., Bryant, P., and Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, Vol. 26, No. 5, pp. 410–417.

Furnell, S. M., Gennatou, M., and Dowland, P.S. (2002). A Prototype Tool for Information Security Awareness and Training. *Logistics Information Management,* Vol. 15, No. 5, pp. 352-357.

Furnell, S. and Thomson, K.-L. (2009). From Culture to Disobedience: Recognising the Varying User Acceptance of IT Security. *Computer Fraud & Security,* Vol. 2009, No. 2, pp. 5-10.

Galvez, S. M., and Guzman, I. R. (2009). Identifying Factors that Influence Corporate Information Security Behavior. Proceedings of the 15th American Conference on Information Systems (AMCIS), USA, California, San Francisco, Paper 765.

Gaston, S.J. (1996). Information Security: Strategies for Successful Management. Toronto: CICA Publishing.

Gefen, D., and Straub, D. (2005). A Practical Guide to Factorial Validity Using PLS Graph: Tutorial and Annotated Example. *Communications of the AIS,* Vol. 16, pp. 91-109.

Gibbs, J. P. (1975). Crime, Punishment, and Deterrence Elsevier, New York.

Glaser, B. G., and Strauss, A. L. (1967). The discovery of grounded theory. Chicago, Aldine Publishing Company.

Glenn, D., G. J. Browne, J. C. Wetherbe. (2006). Why do Internet users stick with a specific web site? A relationship perspective. *International Journal of Electronic Commerce,* Vol. 10, No. 4, pp. 105–141.

Goel, S., and Shawky, H. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, Vol. 46, No. 7, pp 404–410.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, Vol. 19, No. 1, pp. 33–56.

Goucher, W. (2008). Getting the most from training sessions: the art of raising security awareness without curing insomnia. *Computer Fraud & Security*, No. 4, p. 15.

Greaves, M., Zibarras, L. D., Stride, C. (2013). Using the theory of planned behavior to explore environmental behavioral intentions in the workplace. *Journal of Environmental Psychology*, Vol. 34, pp. 109–120.

Greitzer, F. L., Kuchar, O. A., and Huston, K. (2007). Cognitive Science Implications for Enhancing Training Effectiveness in a Serious Gaming Context. *ACM Journal on Educational Resources in Computing*, Vol. 7, No. 3, Article 2.

Gudergan, S.P., Ringle, C.M., Wende, S., and Will, A. (2008). Confirmatory Tetrad Analysis in Pls Path Modeling. *Journal of Business Research*, Vol. 61, No. 12, pp. 1238–1249.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, *Journal of Management Information Systems,* Vol. 28, No. 2, pp. 203–236.

Haeussinger, F., and Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Proceedings of the 15th International Conference on Information Systems (ICIS), Italy, San Milan, Paper 1149.

Hagen, J. M., and Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, Vol. 17, No. 5, pp. 388–407.

Hagger, M. S., Chatzisarantis, N., and Harris, J. (2006). The Process by Which Relative Autonomous Motivation Affects Intentional Behavior: Comparing Effects Across Dieting and Exercise Behaviors. *Motivation and Emotion*, Vol. 30, No. 4, pp. 306–320.

Hagger, M. S., and Chatzisarantis, N. L. (2009). Integrating the theory of planned behaviour and self-determination theory in health behaviour: a meta-analysis. *British Journal of Health Psychology*, Vol. 14, No. 2, pp. 275–302.

Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. (1998). Multivariate Data Analysis. Englewood Cliffs, NJ, Prentice Hall.

Hair, J., Sarstedt, M., Ringle, C., and Mena, J. (2012). An Assessment of the Use of Partial Least Squares Structural Equation Modeling. *Marketing Research, Journal of the Academy of Marketing Science*, Vol. 40, No. 3, pp. 414–433.

Hansche, S. (2001a). Designing a security awareness program: Part 1. *Information Systems Security*, Vol. 9, No. 6, pp. 14–22.

Hansche, S. (2001b). Information System Security Training: Making it Happen, Part 2. *Information Systems Security,* Vol. 10, No. 3, pp. 51–70.

Hawkins, S., Yen, D. C. and Chou, D. C. (2000). Awareness and Challenges of Internet Security. *Information Management & Computer Security,* Vol. 8, No. 3, pp. 131–143.

Heikka, J. (2008). A Constructive Approach to Information Systems Security Training: An Action Research Experience. Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Canada, Ontario, Toronto, pp. 1–8.

Helisch, M., and Pokoyski, D. (2009). Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden, Vieweg Teubner.

Hellqvist, F., Ibrahim, S., Jatko, R., Andersson, A., and Hedström, K. (2013). Getting their Hands Stuck in the Cookie Jar – Students' Security Awareness in 1:1 Laptop Schools. *International Journal of Public Information Systems*, Vol. 2013, No. 1, pp. 1–19.

Hentea, M. (2005). A Perspective on Achieving Information Security Awareness. Informing Science: *International Journal of an Emerging Transdiscipline,* Vol. 2, pp. 169–178.

Herath, T., and Rao, H. R. (2009a). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*, Vol. 47, No. 2, pp. 1–12.

Herath, T., and Rao, H. G. (2009b). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems,* Vol. 18, No. 2, pp. 106–125.

Hofstede, G. (1993). Cultural constraints in management theories. *Academy of Management Executive*, Vol. 7, No. 1, pp. 81–94.

Houghton Mifflin. (2000). The American Heritage Dictionary of the English Language (4th ed.). Boston, MA, Houghton Mifflin.

Hu, Q., and Dinev, T. (2005). Is Spyware an Internet Nuisance or Public Menace? *Communications of the ACM*, Vol. 48, No. 8, pp. 61–66.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, Vol. 54. No. 6, pp. 54–60.

Hurt, H. T., Joseph, K., and Cook, C. D. (Fall, 1977). Scales for the measurement of innovativeness. *Human Communication Research*, Vol. 4, No. 1, pp. 58–65.

ISF (2007). The Standard of Good Practice for Information Security. Information Security Forum, retrieved from https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf.

ISO/IEC 27001 (2005, 2013). Information Technology-Security Techniques – Information Security Management System-Requirements.

ISO/IEC 27002 (2005, 2013). Information Technology-Security Techniques – Code of Practice for Information Security Management.

Jan, A. U., and Contreras, V (2011). Technology acceptance model for the use of information technology in universities. *Computers in Human Behavior*, Vol. 27, No. 2, pp. 845–851.

Jarvis, C., Mackenzie, S., and Podsakoff, P. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research,* Vol. 30, No. 2, pp. 199–218.

Jenkins, J. L., Durcikova, A., and Burns, M. (2011). Get A Cue On IS Security Training: Explaining The Difference Between How Security Cues And Security Arguments Improve Secure Behavior. Proceedings of the 32nd International Conference on Information Systems (ICIS), China, Shanghai, Paper 8.

Jenkins, J. L., Durcikova, A., Ross, G., and Nunamaker Jr, J. F. (2010). Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior. Proceedings of the 31st International Conference on Information Systems (ICIS), USA, Missouri, Saint Louis.

Johnson, E. (2006). Security awareness: Switch to a better programme. Network Security, pp. 15 – 18.

Johnson, M. E. (2011). The Impact of security practices on regulatory compliance and security. Proceedings of the 32nd International Conference on Information Systems (ICIS), China, Shanghai, Paper 6.

Johnson, M. D., Herrmann, A., and Huber, F. (2006). The Evolution of Loyalty Intentions. *Journal of Marketing,* Vol. 70, No. 2, pp. 122–132.

Johnson, D., and Koch, H. (2006). Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?. Proceedings of the 39th Hawaii

International Conference on System Sciences (HICSS), IEEE, USA, Hawaii, Kauai, Vol. 6, pp. 1–9.

Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Mis Quarterly,* Vol. 34, No. 3, pp. 549–566.

Jones, D. (2007). Low Cost Security Tools: Employee Awareness. *Security: Solutions for Enterprise Security Leaders*, Vol. 44, No. 11, pp. 90–91.

Jouini, M., Rabai, L. B., Aissa, A. B. (2014). Classification of Security Threats. *Procedia Computer Science*, Vol. 32, pp. 489–496.

Kam, H., and Katerattanakul, P. (2014). Out-Of-Class Learning: A Pedagogical Approach of Promoting Information Security Education. Proceeding of the 20th Americas Conference on Information Systems (AMCIS), USA, Georgia, Savannah, pp. 1–12.

Kankanhalli, A., Teo, H. H., Tan, B. C., and Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, Vol. 23, No. 2, pp. 139–154.

Karjalainen, M. and Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches*. Journal of the Association for Information Systems,* Vol. 12, No. 8, pp. 518–555.

Katsikas, S. K. (2000). Health care management and information systems security: awareness, training or education?. *International Journal of Medical Informatics*, Vol. 60, No. 2, pp. 129–135.

Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of Information Security Awareness Methods based on Psychological Theories. *African Journal of Business Management*, Vol. 5, No. 26, pp. 10862-10868.

Koskinen, J. A., and Kelo, T. O. (2009). Pure E-learning Course in Information Security. Proceedings of the 2nd International Conference on Security of Information and Networks - SIN '09, North Cyprus, Gazimagusa, pp. 8–13.

Kraiger, K., Ford, J. K., and Salas, E. (1993). Application of cognitive, skill-Based, and affective theories of learning outcomes to new methods of training evaluation. *Journal of Applied Psychology*, Vol. 78, No. 2, pp. 311–328.

Kranz, J., and Haeussinger, F. (2014). Why Deterrence is not enough: The Role of Endogenous Motivations on Employees' Information Security Behavior. Proceedings of the 16th International Conference on Information Systems (ICIS), New Zealand, Auckland, Paper 0520.

Kranz, J. and Picot, A. (2011). Why are Consumers Going Green? The Role of Environmental Concerns in Private Green-IS Adoption. Proceedings of the 19th European Conference on Information Systems, (ECIS), Helsinki, Finland.

Kritzinger, E., and Smith, E. (2008). Information Security Management: An Information Security Retrieval and Awareness model for industry. *Computers & Security,* Vol. 27, No. 5–6, pp. 224–231.

Kruger, H., Drevin, L., and Steyn, T. (2007). Email Security Awareness – a Practical Assessment of Employee Behaviour. Proceedings of the 5th World Conference on Information Security Education (WISE), USA, New York, Westpoint, US Springer, pp. 33–40.

Kruger, H., Drevin, L., and Steyn, T. (2010). A Vocabulary Test to Assess Information Security Awareness. *Information Management & Computer Security*, Vol. 18 No. 5, pp. 316–327.

Kruger, K., and Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security,* Vol. 25, No. 4, pp 289–296.

Kwon, J. and Johnson, M. (2011). The Impact of Security Practices on Regulatory Compliance and Security Performance. Proceedings of 32nd International Conference on Information Systems, (ICIS), China, Shanghai.

Layton, T. P. (2005). Information Security Awareness. Authorhouse, Indiana, Bloomington, p.164.

Leach, J. (2003). Improving User Security Behaviour. *Computers & Security*, Vol. 22, No. 8, pp. 685–692.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013a). Employees' Information Security Awareness and Behavior: A Literature Review. Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 2978–2987.

Lebek, B., Uffen, J., Neumann, M., and Hohler, B. (2013b). Towards A Needs Assessment Process Model For Security, Education, Training And Awareness Programs: An Action Design Research Study. Proceedings of the 22nd European Conference on Information Systems (ECIS). Israel, Tel Aviv, paper 110.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H., (2014). Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, Vol. 37, No. 12, pp.1049–1092.

Lee, D., Larose, R., and Rifon, N. (2008). Keeping Our Network Safe: A Model of Online Protection Behaviour. *Behaviour & Information Technology,* Vol. 27, No. 5, pp 445–454.

Lee, J. and Lee, Y. (2002). A Holistic Model of Computer Abuse within Organizations. *Information Management & Computer Security*, Vol. 10, No. 2, pp. 57–63.

Lee, S. M., Lee, S. G., and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information Management,* Vol. 41, No. 6, pp. 707–718.

Liang, H., Xue, Y., and Wu, L. (2013). Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research*, Vol. 24, No. 2, pp. 279-294.

Liebenau, J., and Backhouse, J. (1990). Understanding information: an introduction. Information Systems, London, UK, Palgrave Macmillan.

Likert, R. (1932). A Technique for The Measurement of Attitudes. *Archives of Psychology,* Vol. 140, pp. 1–55.

Lim, J. S., Ahmad, A., and Maynard, S. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. Proceedings of the 15th Pacific Asia Conference on Information Systems (PACIS), Australia, Brisbane.

Lindell, M. K., and Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, No. 86, pp. 114–121.

Loch, K. D., Straub, D. Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and techological culturation. *IEEE Transactions on Engeneering Management,* Vol. 50, No. 1, pp. 45–63.

Malhotra, Y., Galletta, D. F. and Kirsch, L. J. (2008). How Endogenous Motivations Influence User Intentions: Beyond the Dichotomy of Extrinsic and Intrinsic User Motivations*. Journal of Management Information Systems*, Vol. 25, No. 1, pp. 267–300.

Mancha, R., and Dietrich, G. (2007). Development of a Framework for Analyzing Individual and Environmental Factors Preceding Attitude toward Information Security. Proceedings of the 13th Amercian Conference of Information Systems (AMCIS), USA, Colorado, Keystone, Paper 178.

Mani, D., Mubarak, S., and Choo, K. R. (2014). Understanding the Information Security Awareness Process in Real Estate Organizations Using the SECI Model. Proceedings of the 20th Americas Conference on Information Systems (AMCIS), USA, Georgia, Savannah, pp. 1–11.

Manning, M. (2011). When We Do What We See: The Moderating Role of Social Motivation on the Relation Between Subjective Norms and Behavior in the Theory of Planned Behavior. *Basic and Applied Social Psychology*, Vol. 33, No. 4, pp. 351–364.

Mayfield, J., and Mayfield, M. (2012). The Relationship Between Leader Motivating Language and Self-Efficacy: A Partial Least Squares Model Analysis. *Journal of Business Communication*, Vol. 49, No. 4, pp. 357–376.

McAfee (2012). State of Security Survey. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-state-of-security.pdf

McCoy, C., and Fowler, R. T. (2004). You Are the Key to Security': Establishing a Successful Security Awareness Program. Proceedings of the 32nd Annual ACM SIGUCCS Fall Conference on User Service, USA, New York, New York, pp. 346–349.

McElroy, L., and Weakland. E. (2013). Measuring the Effectiveness of Security Awareness Programs. *Educause Research Bulletin*. December 16th, pp. 1–10.

Mitnick, K. D. (2003). Are You the Weak Link?, Harvard Business Review, Vol. 81, No. 4, pp. 18–20.

Moghaddam, A. (2006). Coding issues in grounded theory. *Issues In Educational Research*, Vol 16, No. 1, pp. 52–66

Moore, G. C., and Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research,* Vol. 2, No. 3, pp. 192–222.

Ng, B. Y., and Kankanhalli, A, (2008). Processing Information Security Messages: An Elaboration Likelihood Perspective. Proceedings of the 16th European Conference on Information Systems (ECIS), Ireland, Galway, Paper 113.

Ng, B., Kankanhalli, A., and Xu, Y. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems,* Vol. 46, No. 4, pp. 815-825.

Ng, B. Y., and Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. Proceedings of the 9th Pacific Asia Conference on Information Systems, Thailand, Bangkok.

NIST (2003). Building an Information Technology Security Awareness and Training Program. In M. Wilson (ed.), NIST Special Publication 800–50. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/

NIST (2006). Information Security Handbook: A Guide for Managers. *NIST Special Publication 800-100,* Gaithersburg, MD: National Institute of Standards and Technology. From http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

North, M. M., George, R., and North, S. M. (2006). Computer Security and Ethics Awareness in University Environments: A Challenge for Management of Information Systems. Proceedings of the 44th annual Southeast Regional Conference (ACM SE'06), USA, Florida, Melbourne, pp 434–439.

North, M. M., Perryman, D., Burns, S., North, S. M. (2010). A Comparative Study Of Information Security And Ethics Awareness In Diverse University Environments. *Journal of Computing Sciences in Colleges*, Vol. 25, No. 5, pp. 223–230.

Norton Symantec Cybercrime Report (2013). Available online at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

Nunnally, J. C., (1978). Psychometric Theory. New York, McGraw Hill.

Offor, P., and Tejay, G. (2014). Information Systems Security Training in Organizations: Andragogical Perspective. Proceedings of the 20th Americas Conference on Information Systems (AMCIS) , USA, Georgia, Savannah, pp 1–9.

Okenyi, P. O., and Owens, T. J. (2007). On the Anatomy of Human Hacking. *Information Systems Security,* Vol. 16, No. 6, pp. 302–314.

Olusegun, O. J., and Ithnin, N. B. (2013). People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization. *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 11, No. 8., pp. 57–64.

Pahnila, S., Siponen, M., and Mahmood, A. (2007a). Employees' Behavior Towards Is Security Policy Compliance. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS), IEEE, USA, Hawaii, Big Island, Waikoloa, pp. 156–166.

Pahnila, S., Siponen, M., and Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. Proceedings of the 18th Pacific Conference on Information Systems (PACIS). New Zealand, Auckland.

Parker, D. (1998). Fighting Computer Crime. New York, J. Wiley and Sons.

Payne, S. (2003). Developing security education and awareness programs. *Educause Quarterly*, Vol. 26, No. 4, pp. 49–53.

Peltier, T. R. (2000). How to build a comprehensive security awareness program. *Computer Security Journal*, Vol. 16, No. 2, pp. 23–32.

Peltier, T. R. (2001). Information Security Risk Analysis. New York, Auerbach.

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, Vol. 14, No. 2, pp. 37–48.

Perlroth, N., and Rusli, E.M. (2012). Security start-ups catch fancy of investors. New York Times, Technology Section, August 5.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, Vol. 88, No. 5, pp. 879–903.

Power, R., and Forte, D. (2006). Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security*, Vol. 5, pp.7–10.

Protogerou, C., Flisher, A. J., Wild, L. G., and Aarø, L. E. (2013). Predictors of condom use in South African university students: a prospective application of the theory of planned behavior*. Journal of Applied Social Psychology*, Vol. 43, Issue supplement S1, pp. E23–E36.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness. Doctoral Dissertation, Department of Information Processing Science, University of Oulu, Finland.

Puhakainen, P. and Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *Mis Quarterly,* Vol. 34, No. 4, pp. 757–778.

PWC (2013): Changing the Game - Key Findings From The Global State of Information Security Survey 2013. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf.

PWC (2014): Defending Yesterday - Key Findings From The Global State of Information Security Survey 2014. Retrieved from http://download.pwc.com/ie/pubs/ 2013_ key_findings_from_the_global_state_of_information_security_survey_2014.pdf

Quazi, M. M. (1993). Effective drug-free workplace plan uses worker testing as a deterrent. *Occupational Health Society,* Vol. 62, No. 6, pp. 26–31.

Qudaih, H. A., Bawazir, M. A., Usman, S. H., and Ibrahim, J. (2014). Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization. *International Journal of Computer Trends and Technology (IJCTT)*, Vol. 10, No 4, pp. 180–186.

Rahim, M., Cheo, A., and Cheong, K. (2008). IT Security Expert's Presentation and Attitude Changes of End-Users Towards IT Security Aware Behaviour: A Pilot Study. Proceedings of the 19th Australasian Conference on Information Systems (ACIS), New Zealand, Christchurch, pp. 780–790.

Rantos, K., Fysarakis, K., and Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, Vol. 21, No. 6, pp. 328–345.

Rao, U. H, and Nayak, U. (2014). The InfoSec Handbook. New York, Apress Media LLC.

Rastogi, R., and von Solms, R. (2012). Information Security Service Branding – Beyond Information Security Awareness. *Systemics, Cybernetics and Infomatics,* Vol. 10, No. 6, pp. 54–59.

Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security,* Vol. 27, No. 7–8, pp. 241–253.

Rhee, H.-S., Kim, C., and Ryu, Y.U. (2009). Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. *Computers & Security,* Vol. 28, No. 8, pp. 1–11.

Ringle, C. M., Wende, S., and Will, A. (2005). Smartpls. Hamburg, Germany, Smart PLS.

Rogers, R. W. (1975). A protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology: Interdisciplinary and Applied,* Vol. 91, No. 1, pp. 93–114.

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory. Social Psychophysiology, New York, J. Cacioppo and R. Petty (Eds.), Guilford.

Rogers, E. M. (1995). Diffusion of Innovations. New York, The Free Press.

Rotvold, G. (2008). How to create a security culture in your organization. *The Information Management Journal*, Vol. 42, No. 6, pp. 32–38.

Rotvold, G. M., and Braathen, S. J. (2008). Integrating Security Awareness Into Business and Information Systems Education*. Journal of Business and Training Education*, Vol. 17, pp. 8–15.

Rounds, M., Pendegraft, R., Pendegraft, N., and Stone, R. (2008). Student Survey on Computer Security Awareness And Responsiveness. Proceedings of the International Conference on Information Resources Management (CONF-IRM), pp. p. 48.

Ryan, J. E. (2006). A comparison of information security trends between formal and informal environments. Doctoral Dissertation, Auburn University, United States – Alabama, retrieved from ProQuest Digital Dissertations database, (Publication No. AAT 3225287).

Ryan, J. E. (2007). Information Security Awareness: An Evaluation among Business Students with Regard to Computer Self-efficacy and Personal Innovation. Proceedings of the 9th Americas Conference on Information Systems (AMCIS). USA, Florida, Tampa, Paper 251.

Ryan, R. M., and Connell, J. P. (1989). Perceived locus of causality and internalization: examining reasons for acting in two domains. *Journal of Personality and Social Psychology*, Vol. 57, No. 5, pp. 749–61.

Ryan, R. M., and Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being*. American Psychologist*, Vol. 55, No. 1, pp. 68–78.

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*, Vol. 39, No. 4, pp. 60–66.

Sari, P. K., and Candiwan, C. (2014). Measuring Information Security Awareness of Indonesian Smartphone Users. *Telecommunication Computing Electronics and Control (TELKOMNIKA)*, Vol. 1, No. 2, pp. 493–500.

Sarstedt, M., and Wilczynski, P. (2009). More for less? A comparison of single-item and multi-item measures. *Die Betriebswirtschaft,* Vol. 69, No. 2, pp. 211–227.

Schultz, E. (2004). Security Training and Awareness-Fitting a Square Peg in a Round Hole. *Computers & Security*, Vol. 23, No. 1, pp. 1-2.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education,* Vol. 52, No. 1, Elsevier Ltd, pp. 92–100.

Siponen, M. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security,* Vol. 8, No. 1, pp. 31–41.

Siponen, M. (2001). Five Dimensions of Information Security Awareness. *Computers & Society,* Vol. 31, No. 2, pp. 24–29.

Siponen, M., and Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *The Data base for Advances in Information Systems,* Vol. 38, No. 1, pp. 60–80.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM,* Vol. 52, No. 12, pp. 145–147.

Siponen, M., Pahnila, S., and Mahmood, A. M. (2006). A New Model for Understanding Users' IS Security Compliance. Proceedings of the 11th Pacific Asia Conference on Information Systems (PACIS), Malaysia, Kuala Lumpur, Paper 48.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, Vol. 43, No. 2, pp. 64–71.

Siponen, M., and Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violations. *MIS Quarterly*, Vol. 34, No. 3, pp. 487–502.

Siponen, M., and Vance, A. (2014). Guidelines for Improving the Contextual Relevance of Field Surveys: the case of information security policy violations. *European Journal of Information Systems*, Vol. 23, No. 3, pp. 289–305.

Siponen M, and Willison R. (2009). Information Security Management Standards: Problems and Solutions. *Information & Management,* Vol. 46, No. 5, pp. 267 - 270.

Sobel, M. (1982). Asymptotic intervals for indirect effects in structural euquation models. *Sociological Methodology,* Leinhart, S. (e.d.). San Francisco, Jossy-Bass, pp. 290-312.

Sommers, K., and Robinson, B. (2004). Security awareness Training for Students at Virginia Commonwealth University. Proceedings of the 32nd Annual ACM SIGUCCS Fall Conference on User services, USA New York, New York, ACM, pp. 379–380.

Son, J. and Rhee, H. (2007). Out of Fear or Desire: Why do Employees Follow Information Systems Security Policies? Proceedings of the 13th Americas Conference on Information Systems (AMCIS), USA, Colorado, Keystone, p. 268.

Spears, J. (2006). The Effects of User Participation in Identifying Information Security Risk in Business Processes. Proceedings of the 44th ACM SIGMIS CPR Conference on Computer Personnel Research, USA, California, Pomona, pp. 351–352.

Spears, J., and Barki, H. (2010). User Participation In Information Systems Security Risk Management. *MIS Quarterly,* Vol. 34, No. 3, pp. 503–522.

Spurling, P. (1995). Promoting Security Awareness and Commitment. *Information Management and Computer Security,* Vol. 3, No. 2, pp. 20–26.

Stanton, J. M., Stam, K. R., Mastrangelo, P. R., and Jolton, J. (2005). An analysis of end user security behaviors. *Computers & Security,* Vol. 24, No. 2, pp. 124–133.

Steven, J., and van Wyk, K. (2006). Essential Factors for Successful Software Security Awareness Training. *Security & Privacy*, IEEE, Vol. 4, No. 5, pp. 80–83.

Straub, D. W. (1989). Validating Instruments in Mis Research. *MIS Quarterly,* Vol. 13, No. 2, pp. 147-169.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research,* Vol. 1, No. 3, pp. 255–276.

Straub, D. W., and Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly,* Vol. 14, No. 1, pp. 45–60.

Straub, D. W., and Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly,* Vol. 22, No. 4, pp. 441–469.

Strauss, L. A., and Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Newbury Park, CA, Sage.

Takemura, T. (2010). A quantitative study on japanese workers' awareness to information security using the data collected by web-based survey. *American Journal of Economics and Business Administration*, Vol. 2, No. 1, pp. 20–26.

Takemura, T. (2011). Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviors in Japan. *Journal of Management Policy and Practice*, Vol. 12, No. 3, pp. 27–37.

Takemura, T., and Umino, A. (2009). A quantitative study on Japanese Internet users' awareness to information security: Necessity and importance of education and policy. Proceedings of the World Academy of Science, Engineering and Technology, pp. 638–644.

Talib, S., Clarke, N. L., and Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. Proceedings of the 5th International Conference on Availability, Reliability and Security (ARES), IEEE, pp. 196–203.

The Economist (2014). Special Report Cyber-Security, July 12th – 18th, UK, London, The Economist Group.

Thomson, M. (1999). Making information security awareness and training more effective. Proceedings of the 1st World Conference on Information Security Education (WISE), IFIP TC11 WG11, Sweden, Kista, pp. 1–10.

Thomson, M. E., and von Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security,* Vol. 6, No. 4, pp. 167–173.

Tse W. K., Hui, M. H., Lam, S. T., Mok, Y. C., Tank, K. L., and Yau, X. L. (2013). Education in IT Security: A Case Study in Banking Industry. *Journal on Computing,* Vol. 3., No. 3.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective,* Vol. 17, No. 5–6, pp. 207–227.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2009). Aligning Security Awareness with Information Systems Security Management. Proceedings of the 4th Mediterranean Conference on Information Systems (MCIS), Turkey, Izmir, paper 73.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., and Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, Vol. 18, No. 5, pp. 350–365.

Tu, Z., and Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. Proceedings of the 20th Americas Conference on Information Systems (AMCIS), USA, Georgia, Savannah.

Turban, D. B., Tan, H. H., Brown, K. G., and Sheldon, K. M. (2007). Antecedents and Outcomes of Perceived Locus of Causality: An Application of Self-Determination Theory. *Journal of Applied Social Psychology*, Vol. 37, No. 10, pp. 2376–2404.

Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems*, Vol. 16, No. 2, pp. 130–152.

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*, Vol., 2006, No. 6, pp. 17–19.

Vallerand, R. J. (1997). Toward a hierarchical model of intrinsic and extrinsic motivation. *Advances in Experimental Social Psychology*, Vol. 29, No. 5–6, pp. 271–360.

Vallerand, R. J. (2000). Deci and Ryan's Self-Determination Theory: A view from the hierarchical model of intrinsic and extrinsic motivation. *Psychological Inquiry*, Vol. 11, No. 4, pp. 312–318.

Venkatesh, V. and Brown, S. A. (2001). A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. *MIS Quarterly, Vol.* 25, No. 1, pp 71–102.

Vermeulen, C., and Von Solms, R. (2002). The information security management toolbox – taking the pain out of security management. *Information Management & Computer Security,* Vol. 10, No. 3, pp. 119–125.

von Solms, R. (1998). Information Security Management (3): The Code of Practice for Information Security Management (BS7799). *Information Management & Computer Security*, Vol. 6, No. 5, pp. 224–225.

von Solms R., and von Solms B. (2004). From Policies to Culture. *Computers & Security*, Vol. 23, No. 4, pp. 275–279.

Vroom, C., and von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, Vol. 23, No. 3, pp. 191–198.

Waly, N., Rana, T., and Kamala. M. (2012). Measures for Improving Information Security Management in Organisations: The Impact of Training and Awareness Programmes. Proceedings of the 17th UK Academy for Information Systems Conference (UKAIS), UK, Oxford, Vol. 8.

Webster, J., and Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing A Literature Review. *MIS Quarterly*, Vol. 26, No. 2, pp. XIII-XXIII.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, Vol.* 46, No. 8, pp. 91–95.

Whitman, M. E. (2008). Information Security: Policy, Processes, and Practices. Chapter 6: Security Policy: From Design to Maintenance. Straub, D. W., Goodman, S., and R. Baskerville (eds.), USA, New York, Armonk, M. E. Sharpe, pp. 123–151.

Whitman, M. E., and Mattord, H. (2011). Management of Information Security, (3rd ed.), Thomson Publishing, Course Technology, USA, MA, Boston.

Whitman, M. E., Townsend A. M., and Aalberts. R. J. (2001). Information Systems Security and the Need for Policy. *Information Security Management: Global Challenges in the New Millennium.* Ed. Gurpreet Dhillon. Hershey PA: IGI Global, pp. 10 – 20.

Wiant, T. L. (2003). Policy and its impact on medical record security. Unpublished Doctoral Dissertation, University of Kentucky, Lexington.

Wilson, M., and Hash, J. (2003). Information technology security awareness, training, education, and certification. Communications. October 2003, Available at: http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm.

Winkler, I., and Dealy, B. (1995). Information Security Technology? Don't rely on it. A Case Study in Social Engineering. Proceedings of the 5th Usenix Unix Security Symposium, USA, California, Berkeley.

Wipawayangkool, K. (2009a). Exploring the Nature of Security Awareness: A Philosophical Perspective. *Issues in Information Systems*, Vol. 10, No. 2, pp. 407–414.

Wipawayangkool, K. (2009b). Security Awareness and Security Training: An Attitudinal Perspective. Proceedings of the 40th Southwest Decision Sciences Annual Conference (**SWDSI**), USA, Oklahoma, Oklahoma City, pp. 266–273.

Woon, I. M. Y., Tan, G. W. and Low, R. T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the 26th International Conference on Information Systems (ICIS), USA, Nevada, Las Vegas, pp. 367–380.

Workman, M., Bommer, W. H., and Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours, *Behaviour & Information Technology*, Vol. 28, No. 6, pp. 563–575.

Wunderlich, P., Kranz, J., Totzek, D., Veit, D. and Picot, A. (2013). The Impact of Endogenous Motivations on Adoption of IT-Enabled Services: The Case of Transformative Services in the Energy Sector. *Journal of Service Research* (*Special Issue on IT-Related Service - A Multidisciplinary Perspective)*, forthcoming.

Yayla, A. (2011). Controlling insider threats with information security policies. Proceedings of the 19th European Conference of Information Systems Proceedings (ECIS), Finland, Helsinki, Paper 242.

Yeh, Q. J., and Chang, A. J. T. (2007). Threats and Countermeasures for Information System Security: A Cross-Industry Study. *Information & Management,* Vol. 44, No. 5, pp. 480–491.

Yiu, T. W., Cheung, S. O., and Siu, L. Y. (2012). Application of Bandura's Self-Efficacy Theory to Examining the Choice of Tactics in Construction Dispute Negotiation. *Journal of Construction Engineering and Management*, Vol. 138, No. 3, pp. 331–340.