5-15-2012

EXPLORING ANTECEDENT ENVIRONMENTAL AND ORGANIZATIONAL FACTORS TO USER-CAUSED INFORMATION LEAKS: A QUALITATIVE STUDY

Frank Hadasch
University of Mannheim

Benjamin Mueller
University of Mannheim

Alexander Maedche
University of Mannheim

EXPLORING ANTECEDENT ENVIRONMENTAL AND ORGANIZATIONAL FACTORS TO USER-CAUSED INFORMATION LEAKS: A QUALITATIVE STUDY[1]

Hadasch, Frank, Chair of Information Systems IV, University of Mannheim, L 15, 1-6, 68131 Mannheim, Germany, hadasch@eris.uni-mannheim.de

Mueller, Benjamin, Chair of Information Systems IV, University of Mannheim, L 15, 1-6, 68131 Mannheim, Germany, mueller@eris.uni-mannheim.de

Maedche, Alexander, Chair of Information Systems IV, Institute for Enterprise Systems, University of Mannheim, L 15, 1-6, 68131 Mannheim, Germany, maedche@eris.uni-mannheim.de

Abstract

Sensitive company information can leak to unauthorized parties in case employees do not perform effective protective measures while using application systems for their day-to-day tasks. To reduce the risks for such information leakage incidents, many companies require their employees to follow information systems (IS) security policies and promote awareness programs to increase IS security awareness. The design of effective IS security awareness approaches is addressed by existing research. However, understanding how environmental and organizational factors influence organizations individuals' IS security awareness is limited. Using grounded theory as qualitative research approach we collect empirical data from 22 informants. The interview data of company outsiders and company insiders is analyzed to identify contextual factors and explain associations among them. Our stated propositions help to understand why individuals in one organization are well aware of IS security threats and policies, while another organization's individuals have a lower level of IS security awareness.

Keywords: Information leaks, security awareness, environmental factors, organizational factors.

[1] We thank the two anonymous reviewers, editor, and track chair for their insightful comments during the development of the manuscript. This work was funded by the DFG (German Research Foundation) under the project User-Centric Information Flow in Enterprise Systems (USIFES) as part of the priority program 1496 "Reliably Secure Software Systems - (RS3)".

1 Introduction

Employees handle sensitive company information in their day-to-day jobs when using application systems. When they store or transmit information in an insecure manner, vulnerabilities that can be exploited by criminal offenders causing information leaks are created (Willison and Backhouse, 2006). While processing sensitive company information users may act with malicious intentions (such as information theft, sabotage, or destruction) or they may perform unintentional or accidental actions, which create risk to confidential information (Warkentin and Willison, 2009; Loch et al., 1992). An example for an unintentionally caused information leakage incident is the loss of detailed personal information of 25 million British citizens in the governmental tax agency. In this incident, 40% of the British population's personal information was leaked caused by "junior" staff members sending password protected but unencrypted hard disks via a private delivery service (Pfanner, 2007). Information leakage incidents can severely impact companies' market value or result in financial losses due to decreased market shares (Acquisti et al., 2006). To reduce the risk of user-caused information leaks, most companies define, communicate, and execute IS security policies with the objective to promote acceptable user actions and prevent unacceptable actions.

Assuming that such IS security policies effectively prescribe secure user actions (Siponen, 2000), most behavioral information systems (IS) security studies investigate individual factors explaining users' compliance or noncompliance with IS security policies (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath and Rao, 2009; Pahnila et al., 2007; Straub, 1990). Their results suggest that IS security policy compliance is anteceded by a variety of different factors. For example, an individual's natural disposition strongly impacts the behavioral intention to comply with IS security policies via mechanisms such as neutralization (Siponen and Vance, 2010). Moreover, and in line with other areas of IS research, also attitude plays an important role in the formation of a user's behavioral intentions in the IS security context (Bulgurcu et al., 2010). Here, particular attention has been devoted to the centrality of security awareness in forming the behavioral intentions to comply with security policies (Dinev and Hu, 2007). In order to create or increase security awareness, mechanisms such as trainings can be used (Puhakainen, 2006; Puhakainen and Siponen, 2010) and create an important complement that is at the discretion of executives responsible for IS security. However, studies on theoretical explanations that could help to inform practitioners in their design of mechanisms to increase IS security awareness (ISA) have hitherto focused on individual factors. In contrast to that, factors on other levels that antecede individuals' ISA lack extensive investigation. But, as highlighted by Stanton et al. (2004), closing this gap between a relevant requirement in practice and the theoretical knowledge explaining security behavior in particular settings is important to design meaningful organizational and technological interventions. Such knowledge can be used to leverage the effectiveness of security trainings or campaigns as well as for the design of technologies preventing information leakage.

It is this ongoing discourse that our study is intended to be a part of. As such, we go beyond the individual level and are seeking to identify contextual factors inside and outside of organizations that impact individuals' ISA. We believe that factors rooted in the organization an individual is part of, or the environment both are embedded in, add important discrete context that helps to better understand and explain individuals' ISA (Johns, 2006). In our work we thus address the following research question: *What are the antecedent environmental and organizational contextual factors that influence an employee's ISA*?

To do so, we are relying on a study design based on the grounded theory method (Corbin and Strauss, 1990; Urquhart et al., 2010) to stimulate the inductive emergence of theory. Encouraged by Johns (2006), we use a set of qualitative interviews to study events of unintentional or accidental information leakage in order to identify environmental and organizational contextual factors. The resulting contributions will be important to understand which role environmental and organizational context play in explaining why individuals in one organization are well aware of IS security threats and policies while another organization's individuals have a lower level of ISA. Ultimately, we argue, this

helps to better understand employees' behavior and how to influence it in order to avoid unintentional or accidental actions, which threaten the confidentiality of information in a work setting.

The remaining parts of this paper are organized as follows: we first review organizational IS security literature. We then present the research method used in section three followed by the study's findings in section four. Finally, we conclude by summarizing key findings and implications.

2 Related work

To understand IS security behavior in organizations current literature examines a variety of factors. Existing studies examine the antecedent factors for IS security management effectiveness (Chang and Ho, 2006; Kankanhalli et al., 2003; Goodhue and Straub, 1991), general security practices (Stanton et al., 2004), or security behavior in academic settings (Kolkowska, 2011).

Chang and Ho (2006) examine the influence of organizational factors on the effectiveness of implementing an information security management standard. Their results reveal that there is a significant impact of various factors, including IT competence of business managers, environment uncertainty, industry type, and organization size on the effectiveness of implementing information security management. Kankanhalli et al. (2003) study if IS security effectiveness is based on organizational factors such as organizational size, top management support, and industry type. They find strong top management support positively influences preventive measures and financial organizations undertake more deterrent efforts toward security. Their findings in regards to the industry type are consistent to the results of Goodhue and Straub (1991). However, existing studies on security management effectiveness lack explaining contextual factors from the environmental and organizational context influencing employees' ISA. Stanton et al. (2004) conduct two national survey studies and explore "some of the motivational antecedents surrounding the practices of information security by end users" (Stanton et al., 2004, p. 1). They report in their study how users' password management and password sharing behavior varies substantially across different industry types. Results reveal that organization size and industry type show relations to some key security behaviors of users. Employees in larger organizations and employees from the military, financial institutions, and telecommunication companies, report better password management practices than employees in other organization types. The suggested model helps to measure outcome variables on password management, but insights into antecedents to ISA are missing. Kolkowska (2011) studies IS security behavior in an academic environment. One of her main finding is that subcultures exist in organizations and that group's value systems predict differences in behavior. Her findings are important to understand how to cultivate different security cultures in organizations. However, as she indicates findings cannot be generalized beyond an academic environment.

Present knowledge on environmental and organizational contextual factors influencing IS security behavior is limited to explaining security management, general security practices, or behavior in academic settings. However, knowledge on antecedents to the theoretical construct ISA is limited, but would be important since latest findings highlight ISA as an important determinant of employees' policy-compliant behavioral intentions (Bulgurcu et al., 2010; Dinev and Hu, 2007; Liang and Xue, 2010; Pahnila et al., 2007). Addressing this lack of understanding is pointed out by Bulgurcu et al. (2010, p. 543) as essential, because "factors that lead to ISA would be an important contribution to academics, since there is a gap in the literature in this direction." For practitioners interested in reducing the risk of information leakage incidents by leveraging the overall security policy-compliance of employees, a clear understanding of possible factors that increase individuals' ISA is important. With this understanding, better organizational interventions (e.g. trainings, campaigns, managerial practices) or technological interventions (e.g. information leakage prevention, violation detection) can be designed that successfully change employees' behaviors in real-world settings (Puhakainen and Siponen, 2010). The lack of theoretical insights into antecedents of ISA, the shown success of interventions in real-world settings that change security behaviors by increasing ISA, and the opportunity to further leverage intervention's effectiveness, urge us to address this gap.

3 Methodology

To provide initial categories for the building of cumulative theory in this area, we follow an inductive theory building strategy to develop a theory for explanation (Gregor, 2006). For the discovery and initial building of substantive theories, the literature discusses a broad range of potential research strategies and approaches. Among them, the grounded theory approach, originally suggested by Glaser and Strauss (1967), has been described as one of the most influential paradigm in the social sciences (Denzin, 1997). The different strands of grounded theory – either as a general approach for theory emergence or as a more formal conception of extracting knowledge from data – are established research approaches in the IS field (Urquhart et al., 2010). For our work, we focus on the more formal grounded theory method perspective suggested by Corbin and Strauss (2007). We perform data analysis during the data collection and follow a theoretical sampling strategy to decide on analytical grounds where to sample from next (Urquhart et al., 2010). This selection process ensures that the substantive area addressed is kept similar and that emerging observations by various respondents are likely to replicate or extend the emergent theory (Orlikowski, 1993).

In the effort to collect data which provides in-depth insights into different companies independent of industries and organizational context, our research design relies on a phased data collection approach (Myers and Newman, 2007; Myers, 2010). To collect industry-independent data first, we designed our study to collect data from outside informants in order to find criteria guiding the second phase. The second phase aims at interviewing inside key informants that are sampled based on criteria identified in the first phase. Inside key informants assess the firm they are employed with. Outside informants such as academics, analysts, and consultants assess the firm of interest from an outer perspective (Chen et al., 1993). The study of Chen et al. (1993) reveals that the reliability and accuracy of outside informants evidences relatively high inter-rater reliability. In their review of 141 studies in the field of strategic management and organizational theory they find academics were most reliable, but less accurate than analysts, which "may be attributable to [academics'] lack of hands-on, in-depth industry knowledge" (Chen et al. 1993, p. 1624).

Following inductive reasoning for theory building based on real-world data, experienced outsiders and inside key informants can be a valuable data source having in-depth industry knowledge and field observations about managers' and employees' behavior. Bernhard et al. (1984) highlight that secondary informants' retrospective cognition about an external reality cannot be genuine proxies for actual behavior. However, we believe to study the sensitive domain of user-caused information leaks informants other than actual employees can be a solid base for rich findings. Under the warrant of strict confidentiality informants can describe the interplay between context and behavior with a high level of accuracy, reliability, and a minimum of socially desirable responses (Trevino, 1992). Grounded in recommendations by Seidler (1974), we do not target at representativeness of employees in a statistical sense, rather, informants are selected due to knowledge about the investigated issue, ability, and willingness to communicate about it (Kumar et al., 1993).

Building on methodological recommendations for instrument development, data gathering, and data analysis in interviews (Lillis, 1999; Schultze and Avital, 2011), we designed and tested a semi-structured interview protocol. Questions on this protocol were for example: What are the most severe information leakage incidents for companies? What is the role of users in such incidents? What are systematic similarities and differences for user-caused information leakage incidents? A copy of the interview guide is available from the first author on request.

We recruited outside informants such as security consultants or computer security forensics. Inside informants have roles such as chief information security officers or computer security forensics. We contacted informants using a global social network for business professionals. The business experts in this network are organized in access-restricted expert groups. Access to an expert group is granted by a moderator upon request based on the applicant's social network profile. We chose a total of three of these groups-of-interest based on a search query involving information security and information

security officer. These search strings are based on the recommendations from a pre-interview with two information security consultants. Adequateness of the chosen groups was assessed by reviewing their titles, self-descriptions, and mission statements as well as analyzing random member profiles.

For one group we isolated a sample of 155 information security professionals based on the social network's industry classification "consulting" (self-reported profile setting). Expert profiles were assessed individually to contact experts with more than four years security experience only. The remaining 113 persons were contacted via the social network's mail function using the profile of one of the authors. Potential informants were asked for a voluntary participation in a telephone interview study on security for future information systems. The correspondence ensured anonymity for the data analysis and mentioned the purpose of the study was to gain better understanding of the general characteristics of information leakage incidents in companies. As an incentive a report for practitioners with the study's results was promised. 16 outsiders volunteered for the telephone interview. Recruiting of inside informants was done accordingly. The number of informants, industry assignment, and informants' average years of experience in the IS security field are summarized in Table 1.

		Outsider		Insider	
Industry	Role	Number of informants	Average years of experience	Number of informants	Average years of experience
Diverse	ISC, CF	14	7.3	-	-
Financial	ISC, CISO, CF	2	8.5	2	7.5
Software/Technology	CISO	-	-	3	5.0
Industrial Equipment	CISO	-	-	1	6.0
	Sum:	16		6	

ISC: Information Security Consultant; CF: Computer Forensic; CISO: Chief Information Security Officer

Table 1. Outside and inside informants recruited for data collection.

The interviews lasted between 90 and 31 minutes with an average duration of 43 minutes. Interviews were tape recorded and transcribed verbatim. Four informants did not agree to tape recording. In these cases the interviewing researcher took notes during the interview. The promised report for practitioners was requested by all participants and mentioned as main motivation for participation. After the interview, the respective transcript was sent to the informant for revision and approval.

Data collection and data analysis were performed in parallel. Previous interviews were used to guide the questions in succeeding interviews. For example, after the first set of eight interviews, clear areas of overlap, redundancy, but also conflicts and inconsistencies began to emerge. At this point results were summarized and the emerging attributes were constantly used in the subsequent interviews to achieve a deeper understanding of the phenomenon (Denison and Mishra, 1995). Based on the analysis and initial findings of outsider interviews, insider informants were selected and interviewed. From the various responses, the systematic similarities and differences are extracted via a process of open, axial, and selective coding (Urquhart et al., 2010; Corbin and Strauss, 2007). For qualitative data analysis (bottom-up open, axial, and selective coding) the software tool MAXQDA was used to assign codes to citations, develop categories and constructs, and to identify relationships among them. The coding was done by the first author and results were reviewed by the other authors as part of the data analysis process to improve inter-rater reliability. Theoretical propositions were developed as part of this process and checked back against the data once the process had reached theoretical saturation.

4 Findings

As part of our data analysis, reoccurring themes of observations, perceptions, and interpretations of informants are grouped into two categories of contextual factors: environmental and organizational. For each of the two categories three contextual factors emerged from the data analysis (Table 2).

Environmental context	Organizational context
Public expectations	Organizational structure
Regulatory requirements	Perception of value of information
Business partner requirements	Communication

Table 2. Contextual factors influencing employees' ISA in company settings.

4.1 Environmental context

One source of input shaping the behavior of an organization's individuals is the organizational environment. Employees' decisions are influenced by the structure of the environment, availability of environmental information, and by respective meaning employees assign to environmental information (Dill, 1958). Originating from the environmental context we find three contextual factors: public expectations, regulatory requirements, and business partner requirements.

4.1.1 Public expectations

Being asked for the kind of information leakage incidents that are most severe for companies, outside and inside informants consistently indicate that maintaining a good public image is a major concern.

> **Outsider security consultant:** Especially those [incidents], which have a certain impact on something. If the public is informed about the loss of data for example. Moreover, in case the image is at stake […].

The public's interest in information leakage incidents seems to put pressure on organizations while the organizations' reaction is dynamic and seems to change over time. A vivid description of such dynamics is given by one freelancing computer forensic as he describes the increasing demand for his services.

> **Outsider computer forensic:** The whole thing has changed through the press of the last months. Our orders really exploded [...] Simply because [the organizations' managers] are afraid that data is being stolen and the main argument was always: *'*We don't want to be in press. Our competitors were in press last week. Please do everything so that this will not happen to us*.'*

To understand which companies perform more actions in regards to IS security than others, informants compared different companies and described their observation.

> **Outsider security consultant:** Companies of course that are on the spot in the market, companies that advertise with their brand, have higher interest in good reputation.

To derive propositions based on these statements, a theoretical anchor can be found in organizational theory. Elsbach and Sutton (1992) describe how companies require legitimacy to act on markets. Legitimacy is conferred when stakeholders endorse and support an organization's goals and activities. Organizational theory stresses the importance of compliance with public expectations, as organizations "will be rewarded for having a legitimate reputation" (Elsbach and Sutton, 1992, p. 700). Murray and Vogel (1997, p. 143) highlight that if "public expectations are ignored and social influence is allowed to take its own course, political and legislative pressure build, frequently leading to negative consequences of the firm." Companies have to deal with social demands and externally imposed expectations to minimize damage to their public image. Stakeholder dissatisfaction builds up when corporate practices do not fulfill societal expectations and the gap between company actions and stakeholder expectations widens as public trust erodes (Murray and Vogel, 1997). We therefore propose:

Proposition 1: The greater an employee's perception of information protection as societal expectation, the higher the perception of publicized leakage incidents as threat to firm's image.

Proposition 2: The greater an employee's perception of good image as competitive advantage, the higher the perception of publicized leakage incidents as threat to firm's image.

4.1.2 Regulatory requirements

In addition to externally imposed public expectations, organizations face heterogeneous institutional regulations (Scott, 1995). Outside and inside informants describe that these regulations influence employee's ISA in companies. For example, a senior security trainer describes his observations in regards to different levels of ISA in various companies.

> **Outsider security consultant:** In case I relate this to sectors, there are sectors with high security awareness, possibly due to legal circumstances, for example the financial sector.

Most informants describe a company's industry as an important attribute when comparing companies in regards to general ISA. However, to identify the reasons for regulatory pressure the scope of laws determine applicability. Refining this, one of the interviewees of our study, who graduated in law and focuses on legal aspects of information protection, highlights that regulatory requirements are based on the type of information being processed in companies rather than on the industry assignment itself.

> **Outsider security consultant (focus on legal aspects):** I think that simply because of the legal requirements there is a higher pressure in the public health sector, especially when sensitive data is processed. [This] type of data brings a certain amount of obligation and responsibility.

Finally, besides the existence of institutional regulations, developing a shared understanding is described as contextual factor influencing ISA.

> **Outsider security consultant:** When I surround a company with sensitive data and develop an understanding that generally we have sensitive data within the company. At a bank for example [I would have this understanding], but if I work in a manufacturing company, it is rather different.

Regulations can be seen as institutional factors that codify widely held beliefs and stem from government initiatives (D'Aunno et al., 2000). Such environmental regulatory policies promote the protection of certain types of company information, for example personal data of customers. Previous studies on IS security behavior find industry type as a determining attribute for general IS security effectiveness (Chang and Ho, 2006; Goodhue and Straub, 1991; Kankanhalli et al., 2003; Stanton et al., 2004). The industry type was mentioned by informants of our study to influence ISA, which is consistent with findings of existing literature. Additionally, we find two further underlying attributes. First, organizations' individuals need to develop a shared understanding of the type of information they process. Second, organizations' individuals need to be able to relate this shared understanding of information types to existing regulations. Therefore we propose:

Proposition 3: The greater an employee's understanding of how regulations apply to the type of information being processed, the higher the perception of publicized leakage incidents as a sanction threat.

4.1.3 Business partner requirements

In addition to factors discussed above, informants described how business partner requirements influence decisions made within organizations. When setting goal attainment for decisions, information about customers, suppliers, and competitors is considered by organizations' individuals (Dill, 1958). An informant working at a small software development company with less than 100 employees explains in which context confidentiality is important.

> **Insider small software vendor:** Especially in the context of communicating with customers it means that sensitive data of some customers need to be encrypted in case the contract requires this.

We compare the answers to an insider of a large software vendor having more than 10,000 employees. This informant confirmed that customer requirements apply to their activities as well.

> **Insider large software vendor:** The most severe [leakage incident] would be, if customer data would be lost, because we provide cloud computing services for our customers. The worst case

would be if data of this customer is in the press or somewhere else [...], customers would cancel contracts and stop cooperation. Then our business would be over.

The answers of both insiders imply that contractual agreements with customers depict influencing factors to the employees' understanding for information protection. As we compared statements of insiders from different company sizes, we propose:

Proposition 4: The greater an employee's understanding of business partner security requirements, the higher the perception of publicized leakage incidents as a threat to the business partner base.

Proposition 5: The impact of employee's understanding of business partner security requirements on the perception of publicized leakage incidents as a threat to the business partner base is independent of company size.

4.2 Organizational context

Originating from the organizational context we find three contextual factors: organizational structure, perception of value of information, and communication.

4.2.1 Organizational structure

Interview partners report about large companies having a better control of their information. To reason why larger companies have a better control of their information, outside informants describe the analysis and definition of business processes as a determining factor.

> **Outsider computer forensic:** Overall, you could say that large companies are rather sensitive with data protection for quite a while. Smaller companies, on the other hand, do not have such a broad awareness. Companies, the large ones actually, are often those that have analyzed and defined their business processes. Those that have a high degree of maturity, are often the ones that better control their data compared to those that do not yet know how exactly a business process works.

In addition our informant describes how organization structures impact the technical enforcement of security policies.

> **Outsider computer forensic:** A strictly hierarchically structured company, a bank for example, adapts its access authorization hierarchically and regulates it strongly.

The analysis of further interviews refines this observation in that the company size itself does not seem to be a determining factor, whereas the structuring of activities in terms of formalization (Pugh et al., 1969) and existing control mechanisms might impact ISA.

> **Outsider security consultant:** Certainly, large companies tend to have more regulations and this is why the awareness could be higher. However, in reality I believe that does not have such a strong impact. This is what I experienced in my projects. Such [lack of ISA] can be found in small as well as in large companies.

Previous studies report that large organizations spend more time and money on security, have more security staff, or have necessary expertise (Kankanhalli et al., 2003). Additionally, our analysis reveals that the reason why larger companies have a higher level of ISA seems to be consistently explained by the degree of formalization of work procedures and number of controls. We therefore propose:

Proposition 6: The greater organizations' formalization of work procedures, the more likely awareness-increasing security controls are in place.

4.2.2 Perceptions of value of information

Employees might value information differently depending on the hierarchical level, type of information, and type of organizational structure (Gallagher, 1974). Employees' perception of the value of information is described by various informants as an important aspect. A IS security trainer

compares an administrative department performing extensive data analysis with a department with minor information processing capabilities.

> **Outsider security consultant:** [Users in this controlling department are] used to perform very intensive and comprehensive data analysis, having a greater insight into business information. They are aware of the consequences associated with this data. [Others do not have such insights.] Especially this lack of knowledge leads to the fact that the value of information is not known.

Beyond an understanding of the value of information, another outside informant describes the importance of understanding threats that are associated with the usage of information systems.

> **Outsider security consultant:** In case [the company's managers] are old fashioned, they see IT as a better typewriter. They do not see the associated threats.

Influence of threat appraisal on security behavior is consistently confirmed in existing IS security literature (Liang and Xue, 2010; Pahnila et al., 2007). Additionally we find the perceived value of information influences the perceived importance of protective measures and therefore suggest:

Proposition 7: The greater an employee's understanding of value of information, the higher the perception of the importance of information protection.

4.2.3 Communication

A shared organizational understanding about the value of information and the importance of protective activities is highlighted by the informants to influence ISA. To achieve a shared understanding, communication is required to transport a set of values and norms that define rules or context for interaction (Leidner and Kayworth, 2006). Norms have an impact on subsequent behaviors of employees and can be either enacted as formal control mechanisms, usually codified in the form of rules and procedures, or through peer influence and the social construction of reality. In an organizational setting formal and social control approaches set expectations and boundaries of appropriate behaviors for organization individuals (O'Reilly and Chatman, 1996).

IS security policies are a form of codifying and communicating a set of rules to define how employees should behave. Informants report that the specification and control of such norms have to be governed by management to legitimate these activities.

> **Outsider security consultant:** The management has to support this, it only works if management implements and controls it from the top. Otherwise there is no chance that it works […].

Furthermore informants describe that an active communication is required to reach out to employees.

> **Outsider security consultant:** [Two banks with similar size] have security policies which disallow [unencrypted data storage]. But as I perceive it, there is a problem with the communication because it is not actively communicated to the employees [in any of the two].

In addition to active communication, an insider describes how persuasive argumentation and multiple channels for communication are used in his organization.

> **Insider security officer:** This awareness you can really only create by giving information to the employees: newsletters, events, such as group meetings, department meetings […] to inform the people: 'Why are we doing this? We are not doing this to boss you around or because we want to control you, but rather we do it because we have agreements with our customers and we have to stick to them. Otherwise our business is endangered.'

Finally, we find that signaling must be consistent to effectively transport messages. O'Reilly and Chatman (1996) describe signaling as a special form of communication in which the transmission occurs through behavior. A manager consistently asking certain questions may send messages about what is important. Behaving inconsistently with existing norms generates signals of conflict.

Outsider security consultant: I have to say in case the management sets an example, it will also work for the employees.

Based on the data analysis in regards to communication as contextual factor we propose:

Proposition 8: The greater an employee's perception of IS security communication being supported by management, the higher the perception of importance of information protection.

Proposition 9: The greater an employee's perception of IS security communication being persuasive, the higher the perception of importance of information protection.

Proposition 10: The lesser an employee's perception of IS security communication conflicts with other signals, the higher the perception of importance of information protection.

Perception of importance and threats ultimately influences individuals' ISA:

Proposition 11: The greater an employee's perception of importance of information protection, the higher an individuals' ISA.

Proposition 12: The greater an employee's perception of environmental context threats, the higher an individuals' ISA.

5 Conclusion

This study identifies three contextual factors originating from environmental context and three contextual factors originating from organizational context that antecede individuals' ISA in particular organizational settings. A lack of ISA among employees is consistently confirmed in existing literature to increase the risk of insecure information processing actions, which could ultimately result in information leaks. Acknowledging these previous findings, our developed propositions describe how public expectations and requirements originate from environmental context. The identified factors influence employees' perception of information leakage incidents as being a threat. As part of the organizational context the formalization of work procedures, employees' perception of value of information, and communication influence individuals' ISA. Employing theoretical sampling and constant comparison we find that the threat perception of lost business partner base is independent of company size. Finally, we find communication can be considered as a crucial aspect to transport understanding of values, norms, and threats among employees. Specifically, the shared understanding among employees is influenced by the way they perceive the role of management and the persuasiveness of communication.

Our study offers practitioners a wide range of recommendations for designing organizational or technological interventions. For example, to increase effectiveness of IS security communication negative consequences of publicized leakage incidents on company's performance should be emphasized. Furthermore, communication should be active, persuasive, use various channels, and minimize signals of conflict. As for the theoretical implications of our work, the suggested categories and propositions can be used as initial stepping stones for the building of cumulative theory improving our understanding of factors influencing individuals' ISA.

When assessing the implications of our work, certain limitations need to be taken into account carefully. One key limitation is the national context the interviews were conducted in. National regulatory requirements and the value dimensions of national culture should be considered as they limit generalization to other contexts. A second key limitation is the selection and number of inside informants. To circumvent socially desired responses to sensitive questions we sampled security officers and forensics asking about their observations and opinions of user behavior. However, we acknowledge interviews with actual users are required to verify our suggested propositions.

Future research can be informed by our research to refine or test the propositions to produce a deeper understanding of how factors relate to each other. To further extend knowledge, in-depth case studies can be conducted to understand why ISA approaches are effective only in particular organizational settings while they are not in others.

References

Acquisti, A., Friedman, A., and Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. *ICIS 2006 Proceedings*, Paper 94.

Bernard, H. R., Killworth, P., Kronenfeld, D., and Sailer, L. (1984). The Problem of Informant Accuracy: The Validity of Retrospective Data. *Annual Review of Anthropology*, *13*, 495–517.

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*, *34*(3), 523–548.

Chang, S. E., and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361.

Chen, M.-J., Farh, J.-L. L., and MacMillan, I. C. (1993). An Exploration of the Expertness of Outside Informants. *The Academy of Management Journal*, *36*(6), 1614–1632.

Corbin, J., and Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, *13*(1), 3–21.

Corbin, J., and Strauss, A. (2007). Basics of qualitative research: grounded theory procedures and techniques. *Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA, USA: Sage.

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*, *20*, 79–98.

D'Aunno, T., Succi, M., and Alexander, J. A. (2000). The Role of Institutional and Market Forces in Divergent Organizational Change. *Administrative Science Quarterly*, *45*(4), 679–703.

Denison, D. R., and Mishra, A. K. (1995). Toward a theory of organizational culture and effectiveness. *Organization Science*, *6*, 204–223.

Denzin, N. K. (1997). Coffee with Anselm. *Qualitative framily research*, *11*(1), 16–18.

Dill, W. R. (1958). Environment as an Influence on Managerial Autonomy. *Administrative Science Quarterly*, *2*(4), 409–443.

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*, *8*(7), 386–408.

Elsbach, K. D., and Sutton, R. I. (1992). Acquiring Organizational Legitimacy through Illegitimate Actions: A Marriage of Institutional and Impression Management Theories. *Academy of Management Journal*, *35*(4), 699–738.

Gallagher, C. A. (1974). Perceptions of the Value of a Management Information System. *The Academy of Management Journal*, *17*(1), 46–55.

Glaser, B. G., and Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research* (1st ed.). Chicago, IL, USA: Aldine.

Goodhue, D. L., and Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information and Management*, *20*(1), 13–27.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642.

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

Johns, G. (2006). The Essential Impact of Context on Organizational Behavior. *Academy of Management Review*, *31*(2), 296–208.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154.

Kolkowska, E. (2011). Security Subcultures in an Organization - Exploring Value Conflicts. *ECIS 2011 Proceedings*, Paper 237.

Kumar, N., Stern, L. W., and Anderson, J. C. (1993). Conducting Interorganizational Research Using Key Informants. *The Academy of Management Journal*, *36*(6), pp. 1633–1651.

Leidner, D. E., and Kayworth, T. R. (2006). Review: A Review of Culture in Information Systems

Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, *30*(2), 357–399.
Liang, H., and Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.
Lillis, A. M. (1999). A framework for the analysis of interview data from multiple field research sites. *Accounting & Finance*, *39*(1), 79–105.
Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, *16*(2), 173–186.
Murray, K. B., and Vogel, C. M. (1997). Using a hierarchy-of-effects approach to gauge the effectiveness of corporate social responsibility to generate goodwill toward the firm: Financial versus nonfinancial impacts. *Journal of Business Research*, *38*(2), 141–159.
Myers, M. D. (2010). *Qualitative Research in Business & Management* (2nd ed.). London, UK: Sage.
Myers, M. D., and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*, 2–26.
O'Reilly, C. A., and Chatman, J. A. (1996). Culture as Social Control: Corporations, Cults, and Commitment. *Research in Organizational Behaviour*, *18*, 157–200.
Orlikowski, W. J. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly*, *17*(3), 309–340.
Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *HICSS 2007 Proceedings* (pp. 156–166).
Pfanner, E. (2007, November 22). Data Leak in Britain Affects 25 Million. *The New York Times*. Retrieved from http://www.nytimes.com/2007/11/22/world/europe/22data.html
Pugh, D. S., Hickson, D. J., Hinings, C. R., and Turner, C. (1969). The Context of Organization Structures. *Administrative Science Quarterly*, *14*(1), 91–114.
Puhakainen, P. (2006). *A design theory for information security awareness*. University of Oulu, FI.
Puhakainen, P., and Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757–778.
Schultze, U., and Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*, 1–16.
Scott, W. R. (1995). *Institutions and Organizations*. Thousand Oaks, CA: Sage.
Seidler, J. (1974). On using informants: A technique for collecting quantitative data and controlling measurement error in organization analysis. *American Sociological Review*, *39*(12), 816–831.
Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.
Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502.
Stanton, J. M., Stam, K. R., Mastrangelo, P. R., and Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. *Proceedings of the Tenth Americas Conference on Information Systems*. New York, NY, USA.
Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276.
Trevino, L. K. (1992). Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations. *Business Ethics Quarterly*, *2*(2), 121–136.
Urquhart, C., Lehmann, H., and Myers, M. D. (2010). Putting the "theory" back into grounded theory: guidelines for grounded theory studies in information systems. *Information Systems Journal*, *20*(4), 357–381.
Warkentin, M., and Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101–105.
Willison, R., and Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403–414.