The Closer You Get the More Aware You Become – A Case Study about Psychological Distance to Information Security Incidents

Lennart Jaeger
German Graduate School of Management and Law, lennart.jaeger@ggs.de

Clara Ament
Goethe-Universität Frankfurt am Main Fachbereich 02 Wirtschaftswissenschaften, ament@wiwi.uni-frankfurt.de

Andreas Eckhardt
German Graduate School of Management and Law (GGS), andreas.eckhardt@ggs.de

Follow this and additional works at: http://aisel.aisnet.org/icis2017

Jaeger, Lennart; Ament, Clara; and Eckhardt, Andreas, "The Closer You Get the More Aware You Become – A Case Study about Psychological Distance to Information Security Incidents" (2017). ICIS 2017 Proceedings. 11.
http://aisel.aisnet.org/icis2017/Security/Presentations/11

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2017 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
The Closer You Get the More Aware You Become – A Case Study about Psychological Distance to Information Security Incidents

Completed Research Paper

Lennart Jaeger
German Graduate School of Management and Law
Am Bildungscampus 2
74076 Heilbronn, Germany
lennart.jaeger@ggs.de

Clara Ament
Goethe-University Frankfurt
Theodor-W.-Adorno-Platz 4
60486 Frankfurt, Germany
ament@wiwi.uni-frankfurt.de

Andreas Eckhardt
German Graduate School of Management and Law
Am Bildungscampus 2
74076 Heilbronn, Germany
andreas.eckhardt@ggs.de

Abstract

Although the increasing number of information security incidents is causing great concern to organizations, their effects on employees’ information security awareness (ISA) are largely left unobserved. Thus, we conduct a qualitative exploratory study in a large financial institution to explore how psychological distance to such incidents influences employees’ ISA. Drawing from construal level theory and interview data from 52 employees we develop a model proposing that ISA can arise due to a lowering temporal, spatial, social, or hypothetical distance towards security incidents. Further, we propose that psychological distance may decrease with the presence of security champions or may increase with employees’ responsibility shift to others. Besides advancing the understanding of how employees construe security incidents, which triggers ISA depending on the perceived distance or proximity, we also offer organizations recommendations for security communication by proposing to manipulate distance dimensions or to artificially recreate such events for raising ISA.

Keywords: Information security awareness, psychological distance, security incident, information security champion, responsibility shift, case study

Introduction

Cybercriminals have spread phishing emails for almost three decades now and security experts expect the problem to get even worse. As such, Jeh Johnson, the Secretary of Homeland Security, rates phishing as a top security threat (Matthews 2016). And there is a simple reason for it: The majority of information security incidents is attributed to the (often unaware) behavior of organizational insiders, i.e. employees with legal access to organizational information systems (IS), who keep falling for phishing attacks (Guo 2013). According to recent reports, in the year 2017, even the tech giants Facebook and Google were
victims of a recent $100m payment scam caused by a Lithuanian hacker (Roberts 2017). Thus, a single email sent to a single user with the right access to an organization’s servers can lead to a mass of encrypted data being held for ransom. In addition to financial losses (e.g., paying for ransom), further negative long-term effects (e.g., loss of reputation or customer trust) complete the fatal consequences such incidents have on organizations. As solely relying on security software and technologies to fix phishing has been a disaster and turned out to be a failed strategy for companies of all kinds over the last decade, the only effective solution, according to security researchers and practitioners alike, is educating and training staff to accurately identify and report suspicious emails (Matthews 2016).

Although humans can still be fooled, research on the effect of security education, training, and awareness (SETA) programs shows that the right training can serve as a helpful instrument supporting employees on the long way towards protecting a company’s technological infrastructure (Puhakainen and Siponen 2010; Tsohou et al. 2015). SETA programs target reducing deficits in employees’ information security behavior and equip them with information security awareness (ISA), i.e. the knowledge and understanding necessary for security-aware decision-making (Bulgurcu et al. 2010). However, both research and practice point out that the management of ISA and, to achieve its desired results, its transfer to corresponding security behavior still encounters significant challenges, as employees tend to ignore security policies or even intentionally try to bypass them (Lowry and Moody 2015). Thus, there is still room for improving the design and content of such programs (Tsohou et al. 2015).

A step towards the direction to improve these programs could be considering users’ real-life experiences as, for instance, the direct personal confrontation with a cyber-attack via phishing. Here, organizations send out phishing emails to their own employees. Those who get fooled are directed a quick online refresher of information aiming to raise awareness and educate the employee. Unfortunately, these artificially designed incidents are both hard to implement (e.g., in terms of ethical and legal compliance) and questionable concerning their long-term effect after uncovering the training measure towards the user. In order to adjust and strengthen existing security-related programs, a shift of thought towards information security incidents needs to be more prevalent in organizations, as they represent both a threat but also an opportunity at the same time. Based on Schein’s (1993) research on organizational learning we know that organizations as a whole and employees in particular learn best by personally experiencing negative lifetime events, such as an information security incident (Tyre and Orlikowski 1994). However, existent research on the effects of information security incidents on employees’ security-related behavior in general and their ISA in particular is scarce. Few exceptions have considered the question ‘whether’ employees ever had a virus or spyware on their computer (Haeussinger and Kranz 2013) or ‘how many’ information security incidents had been known by students (Zhang and Li 2015). Moreover, research on the variation of how strong and directly employees are affected by an incident does not still exist to date. Further it is still unclear how facilitating conditions, in terms of leaders’ security-related championing, or obstacles as employees’ unwillingness to take responsibilities in security-related topics, may increase or decrease this effect. Thus, within this paper, we observe how employees’ temporal, spatial, social, and hypothetical distance to an information security incident shapes their ISA and how psychological distance is influenced by facilitating conditions such as a security championing supervisor and potential obstacles like employees’ responsibility shift of information security to others within the organization (Siponen 2000). Therewith, we offer a more granular understanding of how employees experience and mentally represent information security incidents drawing from the construal-level theory (CLT) of psychological distance (Trope and Liberman 2010). Hence, our research question is:

RQ: How does the psychological distance towards information security incidents influence employees’ information security awareness?

As research in this field is scant and absent of reliable quantitative measures that fully capture the scope and content of possible findings, we address this research question by using a qualitative exploratory study. Within the study we examined a severe information security incident in a large financial institution. Based on 52 interviews with employees of the organization, we are able to derive six propositions for a research model, which can then be quantitatively tested in a subsequent approach.

The remainder of the paper is structured as follows. Section 2 presents the theoretical underpinnings of our research. Section 3 describes the methodology and Section 4 reports the results of the interviews. We end with discussing the findings and contributions of this research, as well as reporting potential limitations of our approach.
Research Background

This section first examines the related work on antecedents of ISA, followed by an explication of the concept of psychological distance based on construal level theory to elaborate how psychological distance to information security incidents may result in varying levels of users’ ISA.

Antecedents of Information Security Awareness

Employees’ ISA is considered to be a crucial ingredient in the continuous effort to make organizations’ information systems more secure (Straub and Welke 1998; Tsohou et al. 2015). Although no generally accepted definition exists in information security literature, ISA most frequently refers to a cognitive state of mind in which employees recognize the importance of information security, are conscious about its objectives, and pay attention to potential information security risks and threats (Siponen 2000; Straub and Welke 1998; Thomson and Solms 1998). Additional exemplary definitions differentiate between employees’ general knowledge and understanding of security issues as well as their cognizance of their organizations’ information security policies and its implications (Bulgurcu et al. 2010). To capture the different facets determining and improving ISA, research in the IS field has begun examining various factors that can be organized according to their level of origin: individual, organizational, social-environmental, and technological (see Table 1).

<table>
<thead>
<tr>
<th>Individual</th>
<th>Organizational</th>
<th>Social-Environmental</th>
<th>Technological</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer self-efficacy</td>
<td>Management support</td>
<td>Business partner requirements</td>
<td>Just-in-time reminders</td>
</tr>
<tr>
<td>IS knowledge</td>
<td>Organizational structure</td>
<td>Peer behavior</td>
<td>Security warnings</td>
</tr>
<tr>
<td>Level of GPA</td>
<td>Security communication</td>
<td>Public expectations</td>
<td></td>
</tr>
<tr>
<td>Negative experience</td>
<td>Security policy provision</td>
<td>Regulatory requirements</td>
<td></td>
</tr>
<tr>
<td>SETA programs</td>
<td>User participation</td>
<td>Secondary sources</td>
<td></td>
</tr>
<tr>
<td>Value of information</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Antecedents of Information Security Awareness

Antecedents of ISA at the individual-level originate from employees or IS users and include computer self-efficacy (Zhang and Li 2015), general IS knowledge (Haeussinger and Kranz 2013), the level of grade point average (GPA) (Zhang and Li 2015), and personal negative experience with information security incidents (e.g., a virus attack or punishment due to policy non-compliance) (Haeussinger and Kranz 2013). Organizational antecedents of ISA relate to factors under the influence of the organization and largely rely on its security management practices. This includes management’s support of information security initiatives (Hu et al. 2007), organizational structure (e.g., formalization of work procedures in the form of awareness-increasing security controls) (Hadasch et al. 2012), information security communication (Hadasch et al. 2012), security policy provision and promotion (Haeussinger and Kranz 2013), security education, training, and awareness (SETA) programs (Culnan et al. 2008; D’Arcy et al. 2009; Haeussinger and Kranz 2013; Straub and Welke 1998), user participation in security risk management processes (Spears and Barki 2010), and employees’ perception of value of information (Hadasch et al. 2012). Social-environmental antecedents differ in so far from organizational antecedents in that they are not under the direct influence of the organization’s management but originate from organizational IS users’ employee interactions with their social environment. This includes business partners requirements (Hadasch et al. 2012), observing security-related peer behavior (e.g., their policy compliance) (Haeussinger and Kranz 2013) public expectations of information protection and security requirements from regulatory bodies (Hadasch et al. 2012), as well as additional secondary sources (e.g., media information about security issues) (Haeussinger and Kranz 2013). Finally, technological antecedents originate from technical tools with integrated awareness-raising features that were designed and developed with the objective to increase awareness in specific software applications, such as web browsers, by alerting the users to possible information security threats that may arise. Examples include just-in-time reminders in the form of pop-ups as SETA program components (Jenkins and Durcikova 2013) and the frequency of information security warning messages (Zhang and Li 2015).
Summing up, prior research has built a considerable body of knowledge about determinants of ISA but interestingly just little is based on direct life experiences, shaping an employee’s awareness at the forefront (Bulgurcu et al. 2010). Such direct life experiences can be gathered during a SETA program session or during an actual information security incident such as a phishing attack. In particular, an important issue in information security research is the lack of empirical studies on the impact of information security incidents on affected users and their peers (Lee and Lee 2012). As information security incidents are not easy to manipulate and replicate in reality, and independent researchers have rarely access to data about their effects, empirically tested knowledge is scarce and scholars are forced to build theories based on unfounded assumptions. Hence, there is very little empirical evidence about the scope and extent of the impact of information security incidents on employees’ ISA.

**Construal-Level Theory of Psychological Distance**

For explaining how employees form mental representations of an information security incident thus improving our understanding of how psychological distance towards information security incidents impacts employees’ levels of ISA, we apply construal-level theory (CLT).

In terms of CLT an event is seen as psychologically distant when it is outside of the immediate physical experience and must therefore be construed mentally (Trope and Liberman 2010). In this sense, all events that do not occur in the immediate here and now are distant. Individuals experience only themselves as well as the here and now directly and must overcome distance in order to plan for the future, for other persons and remote places, but also for the occurrence of hypothetical events. Psychological distance is represented on four dimensions: temporal, spatial, social, and hypothetical (Bar-Anan et al. 2006; Liberman and Trope 2008). An event is temporally distant when it takes place in the past or in the future (e.g., first professional experience). Spatial distance refers to events located at remote locations (e.g., at another company). Social distance is given, when experiences are not related to oneself, but to others (e.g., a decision for colleagues, relatives or strangers). Hypothetical distance emerges when (supposedly) less probable or unreal events are considered (e.g., a complete breakdown of the communication infrastructure).

The main assumption of CLT is that the cognitive representation of events changes with increasing distance. In doing so, the concreteness or abstractness of the representations changes. At a low psychological distance, more concrete representations (or low-level construals) of events are formed. In the case of high psychological distance, individuals form more abstract representations (or high level construals). A low-level construal represents events concretely, unstructured, and contextualized, whereas a high-level construal is associated with an abstract, schematic, and de-contextualized representation of the same event (Liberman and Trope 2008). The high-level construal thus lies higher on a conceptual hierarchy with respect to centrality, general meaning, and valence (Fiske and Taylor 1991; Smith 1998). For example, a high-level construal of an information security incident would highlight the abstract and organizing essence of this class of events; employees represent an information security incident as a general, abstract category that has certain high-level features (e.g., harm) and as such as an organizational problem. By contrast a low-level conception of information security incidents emphasizes more varied and concrete features of specific realizations; such incidents are considered as a more specific threat, differentiated and potentially tangible in the everyday work of an employee (Trope and Liberman 2010).

Existing research shows that all four dimensions of distance (temporal, spatial, social, and hypothetical) are directly related to one another in cognitive representation (Bar-Anan et al. 2007). Furthermore, it is empirically proven that distance and abstraction levels influence each other. In the same way that higher distance leads to more abstract representations of events, more abstract representations also lead to events being perceived more distantly (Trope et al. 2007).

Overall, empirical research on CLT shows that psychological distance of any kind changes the representation of events with respect to their degree of abstraction in such a way that distant (vs. proximal) entities are constructed as more abstract (vs. concrete). The four distance dimensions, namely temporal, spatial, social, and hypothetical distance, forming together the more comprehensive construct “psychological distance” influence in a similar way how individuals perceive events, evaluate, predict, and also act towards them (Liberman and Trope 2008).
Theoretical Framing: Construal-Level Theory in the Context of Phishing

In order to work out, why CLT of psychological distance might open up new research directions for ISA, we use the example of phishing as an information security incident illustration in the following. Most employees do not experience phishing directly, as victims, however still are able to think, feel, and take action about the risk of becoming a victim. In CLT terms, ISA is a set of representations and perceptions toward the distal event of phishing that is based on psychological distance and mental construal. When the distal event of phishing is perceived as psychologically distant, it is assumed to be experienced by an employee as happening far from now (temporal distance), somewhere else (spatial distance), to other employees than themselves or their close peers (social distance), and is unlikely or unrealistic (hypothetical distance) (Trope and Liberman 2010). Employees will then construe the distal event in high-level terms emphasizing what is at the ‘core’ of the abstract concept of phishing, i.e. its abstract features that do not vary from one realization of information security incidents to another and, as such, may be more easily related to other abstract security problems, like IS misuse or information security policy violations. To the extent that psychological distance to phishing and an abstract, high-level phishing construal will be related to ISA, it may be that ISA is more diffuse knowledge about the consequences and significance of phishing in organizations, rather than more concrete knowledge about how to detect and avoid phishing at one’s own workstation.

Conversely, when employees experience phishing as psychologically proximal, they experience it as occurring soon (temporal proximity), in a nearby location (spatial proximity), to oneself or similar others (social proximity), and as likely or realistic (hypothetical proximity) (Trope and Liberman 2010). CLT predicts that in such cases, people will also construe phishing in a more concrete, specific, and variegated fashion, that is, by focusing on situational features that do vary from one realization of one information security incident to another and, as such, may be more easily related to how phishing can occur through, for instance, malicious websites and email attachments. Psychological proximity to information security incidents and a concrete low-level phishing construal may thus be more likely to involve a perception about one’s own risk of phishing, where the incident is projected to occur sooner rather than later, at one’s own workstation rather than at another company, to one’s self or similar peers rather than different employees, and is rather likely than unlikely.

Whether employees think more abstractly or concretely about phishing is attributed to a shift in purpose (Trope and Liberman 2010). As proximal events like imminent information security incidents (e.g., a phishing attack) require a direct response, employees need to understand ‘how’ they are affected by it. To respond appropriately, employees construct concrete construals with practical details of the specific incident. Their purpose is thus to explain feasibility, i.e. how they can react to the incident. Opposite to this, distant incidents do not demand a direct response but rather a judgment of ‘whether’ they will be affected by it. Consequently, employees construct abstract construals with a focus on the desirability of the incident in abstract terms, i.e. whether it needs to be avoided. By so doing, peripheral features related to feasibility are omitted and central features related to desirability are taken into account (Trope and Liberman 2010).

Methodology

In the subsequent section, the methodology of our investigation is described. Integrating the concept of psychological distance into an information security context is associated with a high degree of uncertainty. Thus, in the absence of reliable quantitative measures, it is adequate to use a qualitative research approach, which is widely accepted in IS literature (Myers 1997; Trauth 2001). We designed and conducted a case study best characterized by a “soft positivistic” approach (Kirsch 2004; Madill et al. 2000). According to this approach, data analysis is conducted with some expectations using an existing theoretical lens, but is also open to obtain new findings and explanations from data, similar to interpretivist or grounded theory approaches (Kirsch 2004; Madill et al. 2000). In our study, the positivist stance gave us the necessary initial focus on psychological distance by using the lens of the construal level theory, while the softer stance enabled us to develop themes and aggregate dimensions, and drawing conclusions about the relationship between psychological distance towards information security incidents and information security awareness.
Context

Our field study was conducted within the financial industry. The case company, hereafter pseudonymized as the Bank, is by asset size one of the largest financial institutions in Europe. It is the central headquarters for one of the largest European financial service organization networks, thereby serving millions of customers. Furthermore, the Bank functions as corporate and investment bank. The majority of IS functionalities are conducted in-house. The Bank's IT department acts as an enabling partner for all business units. Its task portfolio includes, for instance, user management, project management and consulting, datacenter and workstation control, as well as the provision of hardware and software solutions. Of certain interest for our study is the IT management division, where the framework for IT controlling and IT risk management is situated. The IT risk management unit has the responsibility to collect, evaluate and process the operational IT risks and security.

Data Collection

Besides discussions with information security experts, interviews served as the main information source for our field study. In the third quarter of 2016, two researchers interviewed employees at the Bank's headquarters. The research endeavor was supported by the organization’s head of IT, who invited employees throughout all departments to participate in the interviews. The invitation email, which was sent out, emphasized the study’s academic and independent nature. The employees received information on the purpose of the interviews, namely an analysis of information security awareness among employees at the Bank. Besides, to get honest reactions to sensitive subjects, those responsible emphasized that participation was voluntary, anonymous, and confidential (Bennett and Robinson 2000).

In total, we conducted interviews with 52 employees from various levels and units throughout the Bank. This included employees from business units (n = 38), such as operations, payments and accounts, transaction management, or corporate banking, as well as from the IT unit (n = 14) and, among the latter, employees with a certain responsibility for information security (n = 8). We interviewed 33 men and 19 women. The average interviewee was 43 years old and had 20 years of professional experience. Table 2 presents the demographic characteristics of the interviewees.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Highest level of education</th>
<th>Job tenure (in years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>36.5%</td>
<td>Less than high school degree</td>
<td>17.3%</td>
</tr>
<tr>
<td>Female</td>
<td>63.5%</td>
<td>High school degree or similar</td>
<td>21.2%</td>
</tr>
<tr>
<td></td>
<td>20-29</td>
<td>Bachelor degree or similar</td>
<td>3.8%</td>
</tr>
<tr>
<td></td>
<td>30-39</td>
<td>Master degree or similar</td>
<td>55.8%</td>
</tr>
<tr>
<td></td>
<td>40-49</td>
<td>Doctorate degree</td>
<td>1.9%</td>
</tr>
<tr>
<td></td>
<td>50-59</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Demographic Characteristics of Interviewees (n = 52)

All interviews lasted between 30 and 45 minutes. Interviews with employees from other branches, including foreign branches, had to be conducted via telephone. We conducted the interviews in a semi-structured format, as commonly used in IS research (Myers and Newman 2007). This involved a pre-preparation of a guideline, which consisted of three parts. The first part referred to characteristics of the participant (e.g., age, gender, highest level of education, years of work experience, current roles and division at firm). The second part addressed the concept of information security awareness. We asked the interviewees about their understanding of information security awareness as well as central awareness-raising approaches (including their desirability, feasibility, and effectiveness) corresponding to the organizational antecedents of ISA previously identified in our literature review (e.g., SETA programs, security warnings), organizational aspects (e.g., structure), metrics, roles of employees and security experts, their level of involvement in information security, exchanges about information security in the department, challenges and success factors of information security awareness. In the third part we asked the interviewees about information security incidents that have happened in the past, particularly on their background and the whole process, including how they learned about it (e.g., whether it was addressed by their colleagues or supervisors, whether the IS department informed them about it, whether it was a topic in their weekly meetings), how they were personally affected by it, and how it was post-treated. If
participants mentioned a particular incident, we further inquired, whether they knew how often such
incidents happen or might happen again in future, where it happened (e.g., in which subsidiary), whether
it happened to them or colleagues and might happen again. Another focus in the third part was, what kind
of impact this incident had on the employees, for instance, in how far they were sensitized by it towards
information security, whether it changed their behavior, and the level of importance of information
security in their department before the incident as compared to after the incident.

During the whole interview, we invited interviewees to provide examples, anecdotes, and more details on
potentially important topics. With this approach, we could analyze our qualitative data with the necessary
integrity (Wallendorf and Belk 1989). To avoid active listening, questions were phrased in a nondirective
and unobtrusive manner (McCracken 1988). We recorded all interviews digitally and transcribed them
with the permission of the interviewees. Over time, responses from the interviewees became
homogeneous and no new insights emerged, thus, we did not regard further interviews as necessary
(Lincoln and Guba 1985).

Data Analysis

The analysis of transcripts followed an iterative multilevel coding process, which is present in multiple IS
studies (compare, for instance, Charki et al. 2017; Spears and Barki 2010). The transcript analysis was
done with NVivo Pro 11, a qualitative data analysis software package developed by QSR International. The
interviews were coded in several steps. First, during open coding, the data was analyzed line-by-line to
identify relevant concepts based on the actual statements of the interviewees and, as a result, concepts
related in meaning were grouped into first-order concepts (e.g., temporal frequency of information
security incidents, see Table 3).

<table>
<thead>
<tr>
<th>First-order concepts</th>
<th>Second-order themes</th>
<th>Aggregate dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security incidents’ temporal frequency; temporal length; temporal change in frequency</td>
<td>Temporal distance towards information security incidents</td>
<td>Psychological distance towards information security incidents</td>
</tr>
<tr>
<td>Physical distance; virtual distance</td>
<td>Spatial distance towards information security incidents</td>
<td></td>
</tr>
<tr>
<td>Flow of security information; peer behavior observation; previous experience with incidents</td>
<td>Social distance towards information security incidents</td>
<td></td>
</tr>
<tr>
<td>Susceptibility to security incidents; skepticism about security incidents; uncertainty about security incidents</td>
<td>Hypothetical distance towards information security incidents</td>
<td></td>
</tr>
<tr>
<td>General information security awareness</td>
<td>Information security awareness</td>
<td>Information security awareness</td>
</tr>
<tr>
<td>Information security policy awareness; awareness about governmental regulations</td>
<td></td>
<td>Information security awareness</td>
</tr>
<tr>
<td>Awareness about security threats; awareness about security countermeasures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees as security multipliers; group leader as role model; failure-tolerant, empathic leader</td>
<td>Information security champion</td>
<td>Facilitating conditions</td>
</tr>
<tr>
<td>Employees’ reliance on IT infrastructure and department; understanding of roles; convenience versus security</td>
<td>Responsibility shift</td>
<td>Potential obstacles</td>
</tr>
</tbody>
</table>

Table 3. Emergent Concepts, Themes and Dimensions

Next, we used axial coding to contextualize the first-order categories with supplementary literature,
search for relationships among them, and, consequently, to reassemble them into second-order themes
(e.g., temporal distance to information security incidents, see Table 3). Finally, we implemented selective
coding, where all second-order themes were grouped into aggregate dimensions (e.g., psychological distance to information security incidents, see Table 3). From aggregation a new framework emerged, comprising empirically embedded propositions and insights (Corbin and Strauss 2008).

To establish trustworthiness and credibility, we employed principles of data and research triangulation (Lincoln and Guba 1985). For data triangulation, we constantly compared field data (transcripts and memos) with related research on information security awareness and psychological distance. For research triangulation, two scholars carried out each coding stage independently. We frequently and extensively discussed our coding outcomes, and integrated the coding plans after each coding stage.

**Results**

Interviewees reported in detail on a severe incident, which happened two weeks prior to the interviews. Based on various points of view, including the person causing the incident, peers from the same department or affected neighboring units, and the involved information security officers, we subsequently describe the incident as objectively as possible.

The incident occurred as follows. Prepared files were sent to employees of several companies, including our case company, via phishing emails. These files were infected with the “Locky” ransomware, i.e. manipulated excel and voicemail files that upon opening encrypt all files on the computer based on an algorithm and demand a ransom for decrypting them again. This is common practice of attackers today as a review on malware in the first quarter of 2016 reports that 93% of phishing emails were infected with ransomware and nearly 75% of them contained “Locky” (PhishMe 2016). One employee of the Bank opened such an infected file, which as described encrypted all files on his personal workstation. In addition, “Locky” also spread through the Bank’s shared drives and encrypted other computers. Following this, all employees of the affected department were prompted to disconnect their computer from the network and to shut them down. Statements about the exact extent in terms of affected employees and financial damage vary among interviewees, but based on the timing of events more than half a day of working time was lost for 150-200 employees. Formal forms of post-processing the information security incident only stressed how to handle unknown emails and included an email sent to all employees, an intranet message, and a pop-up on all workstations. A plausible explanation why this incident was not communicated more transparently may be attributed to the fact that the Bank underwent a major organizational change the following week. Public knowledge of the information security incident may thus have been considered to have negative consequences.

In the following, we report our results on how psychological distance towards information security incidents influences employees’ levels of ISA. Whether employees experience information security incidents as psychologically proximal or distant was analyzed based on the four dimensions (temporal, spatial, social, and hypothetical) introduced in the research background on CLT.

*Temporal Distance towards Information Security Incidents*

We found that temporal distance towards an information security incident includes the characteristics temporal frequency of information security incidents (never vs. often), temporal length of information security incidents (short vs. long), and temporal change in frequency (decreasing vs. increasing). These findings are in line with CLT reasoning. When the temporal distance towards an event decreases employees experience an event as occurring rather sooner than later (Trope and Liberman 2010). In our study, most employees perceived information security incidents as occurring regularly and with an increasing frequency, while only few have not consciously noticed an information security incident recently. One respondent, for instance, reflected on and predicted how often it may be the case that a harmful link or attachment in an email is being clicked on:

"Just last week our team leader told us that there was such an incident [referring to the Locky ransomware incident]. Besides that? I can imagine that this happens more often to me. Maybe even several times a month. I could imagine that something like this can happen maybe once a week.” (male, 45 years, business unit)

Another respondent added a more cautious guess:
"Two to three times [a year]. I don't know exactly, roughly, I would say. Well, this real Trojan wave [referring to the Locky ransomware incident] like 14 days ago on such a massive scale, I am not aware that this was the case over the last years." (female, 46 years, business unit)

Upon reflecting on their level of ISA, temporarily more proximal interviewees responded that they were more sensitized or developed a sense for phishing emails. One respondent summarized the effect of more frequent events as follows.

"I mean this Trojan [referring to the Locky ransomware] two weeks ago – that was not the first time. But it was now even stronger than the others. Maybe if you had sensitized the people before, maybe you could have prevented it, but I do not know exactly what to do...or how it was already in people's awareness. I believe the more frequent this happens now, the more one is actually prompted to »sh** ok, strange attachment, strange sender« the more you really have learning by doing, so to speak." (female, 28 years, business unit)

Information security incidents that are expected to occur rather sooner than later provoke a more immediate perception about one's own risk of victimization prompting employees to be on alert, for instance while opening unknown emails, and thus being more aware of information security issues. We thus propose:

**Proposition 1**: The lower the temporal distance to information security incidents, the higher employees' level of ISA.

**Spatial Distance towards Information Security Incidents**

When spatial distance towards an event decreases, employees experience it as occurring nearby rather than somewhere else (Trope and Liberman 2010). We find that spatial distance includes the characteristics of physical distance (e.g., in the department or company vs. at other companies) and virtual distance (e.g., at one's own workstation or email box, group disk drive vs. at other computers). Our findings show that the majority of employees perceive that they were or could be directly affected by information security incidents, either at their own workstation, in their department, or at their company. One respondent compared her experience with the Locky ransomware incident to the spatial proximity of terrorist attacks:

"Because this is actually like with the terrorist attacks in Berlin or Brussels were you said »oh sh**, this is not nice but it was nevertheless far away. When, for the first time, one [terrorist attack] was thwarted in [name of the city removed for reasons of anonymity] and you knew this is very close by, you felt somehow rather strange. So transporting this feeling, let me say, consciously, that would be ideal in my opinion." (female, 54 years, business unit)

Another respondent reported, what employees and the organization as a whole should learn from the Locky ransomware incident:

"In particular, to sharpen this information security awareness. You always heard about it but we were never affected by it. Probably this has already happened here in the Bank, but it was never this close." (female, 46 years, business unit)

Spatially more proximal respondents stressed a sensitizing effect on their awareness that was not only related to believing that such incidents are more serious (e.g., their workstation could also become compromised), but also expressed a certain degree of concern that a severe information security incident could happen at their organization. Another respondent summarized the effect of the Locky ransomware incident as follows:

"Our neighboring group was in quarantine. So in that way we had a really, let's say, emergency for the department. That was really annoying. But I would simply expect that the bank's firewall simply keeps something like this away. So that was quite spectacular. But, of course it is sad, that something ends in the spam folder again and again. Okay, I do not find this that bad. The firewall is there for that. But that whole Trojans find their way into the bank that makes you a bit worried." (male, 48 years, business unit)
We argue that information security incidents perceived to occur nearby at one’s own workstation or department rather than at another company make an information security incident more concrete, thereby creating a greater sense of self-risk and prompting employees to be more careful, for instance, with handling their emails. Hence, it follows:

**Proposition 2**: The lower the spatial distance to information security incidents, the higher employees’ level of ISA.

### Social Distance towards Information Security Incidents

When employees experience events as socially proximal (vs. socially distant), they experience it as happening to themselves or similar others (vs. to dissimilar others) (Trope and Liberman 2010). We find that social distance towards information security incidents includes the characteristics of flow of security information (i.e., whether employees heard about incidents through office grapevine vs. through formal security communication in the form of intranet newsletters), peer behavior observation, and own previous experience with incidents. Employees considered being socially proximal towards information security incidents perceived that it could happen to them by causing an incident, being personally affected by it, or knowing close colleagues to whom it happened or may happen. One respondent summarized her previous experience with malware and its effect on her ISA levels as follows:

> “Somehow in this jumble, millions of e-mails, and then I had one and only thought, »what is that?« and somehow before I really thought about it I had already clicked on it. I think I have just said, »No!« and then shut down or whatever. Then it took half a day until they had cleaned my computer again and since then I am in alert and it is now also present.” (female, 48 years, business unit).

In addition to employees’ own experience of being directly or indirectly harmed contributing to a higher self-risk perception, respondents also reported that hearing incidents from close colleagues and acquaintances sensitized them so that they pay more attention towards information security threats.

> “But now you can quite concretely observe such an encryption thing [referring to the Locky ransomware] currently running through the media, also in the wild within your circle of colleagues. I am following this with great interest, how this works at the end and what they do there. For example, I also manage my own backup and security strategies to deal with it and behave accordingly. I inform myself how attack methods like that simply work to protect myself against it.” (male, 34 years, business unit).

This finding also corresponds with previous research proposing that not just the own experience but also hearing of similar or other information security incidents from friends, family members and relatives increases the likelihood to pay attention to information security (Zhang and Li 2015). Thus, we propose:

**Proposition 3**: The lower the social distance to information security incidents, the higher employees’ level of ISA.

### Hypothetical Distance towards Information Security Incidents

When employees experience events as hypothetically proximal (vs. hypothetically distant), they experience it as being likely or realistic (vs. unlikely or unrealistic) (Trope and Liberman 2010). In other words, employees make judgements about an event that has a high or low probability of occurring, and the lower the certainty (or likelihood) associated with the event, the greater its hypothetical distance (Waksalak et al. 2006; Waksalak and Trope 2009). The event of an information security incident would then seem distant when this is an incident one could experience rather than an incident one has experienced, and the lower the likelihood of actually experiencing this incident, the greater its hypothetical distance.

Employees considered as being hypothetically proximal reported that incidents are very likely and could always happen or as one respondent from the business unit put it:

> “We are more than 5000 people and there are so many incoming emails and so many things you also expect, that it can happen very quickly that something slips through.” (male, 45 years, business unit)
Other employees reported on how having experienced the Locky ransomware incident changed their probability judgements on whether future incidents could actually happen.

“I would never have thought that you can get it [referring to the Locky ransomware] in the bank, but one is always wiser after the event, because you cannot be secured against everything. And everybody who works much with a PC at home knows that there is no 100% security.” (male, 48 years, business unit)

Conversely, a high hypothetical distance was characterized by feeling safeguarded as an end-user at the workplace and skepticism of information security incidents actually occurring.

“Well, I assume that the bank takes care and assures us this kind of security in the background. So because of this I assume at least I hope we are acting in a secure environment to begin with.” (female, 46 years old, business unit)

“This is probably not so often because the antivirus software is still there. It can only happen if really all safety measures are really futile.” (male, 48 years, IT unit)

Respondents with a low level of hypothetical distance perceived that employees should always use their common sense and should have at least so much awareness to verify whether unknown emails are truly trustworthy. Conversely, respondents with a high level of hypothetical distance predominantly failed to recognize that having a secured IS infrastructure and firewall is not enough to control for information security incidents caused by employees’ actions. In general terms, when employees perceive information security incidents as almost certain to occur (as opposed to almost certain not to occur), they react to it cognitively in the form of a heightened awareness by paying more attention to information security risks and threats, and developing an interest in how to prevent them. Thus, we propose:

**Proposition 4**: The lower the hypothetical distance to information security incidents, the higher employees’ level of ISA.

**Facilitating Conditions**

We also find that certain factors may reduce the psychological distance to information security incidents. Employees emphasized the importance of information security champions, which are characterized as employees from different departments at different hierarchical levels, who voluntarily take extraordinary interest in information security. For instance, some employees from the business unit, considered themselves to be in a role as a mediator of information security in their department, i.e. as soon as they receive security-related information they spread it among others. This potential multiplying effect was described as follows:

“So I see myself also as a multiplier for such security questions in the sense of [telling people to] »take heed!« or when something goes around in our house.” (female, 52 years, business unit)

Further, answering the question whether he sees himself in the role as a mediator, who points out security threats, a group leader stated:

“Yes, I actually do this. Uh, if this is always successful, remains to be seen. But sometimes for one person or the other, I have certainly created awareness for it, but this is a very lengthy process. This is not so simple somehow.” (male, 48 years, business unit)

Respondents further recognized the important role of a leader as an information security champion, which is attributed to group and department leaders.

“As a matter of fact I do see this as my responsibility as a leading force to do this, and therefore I just do it. Security topics are also the topics of leadership and it has to be exemplified by the leader as well. This is the biggest problem in security. If security measures are not demonstrated and used correctly by the leader, then no one will take them seriously. And living by the standards as a leader means in the end completely and consequently so all the way from the top-level until middle-level leaders and low-level leaders.” (male, 59 years, IT unit)

Going beyond being role models, soft skills seem to be also a necessary requirement for leaders for awakening employees’ information security awareness. Eliminating fears and inhibitions, while making
their approachability and availability clear (i.e. breaking the traditional barrier between boss and subordinate), empathetic leaders strengthen employees’ confidence in themselves and in the company, and at the same time sensitize them.

“He [the leader] should also have a social competence, so that he himself is empathetic towards others when he approaches them and if someone calls him anxiously, that he won’t just say »Oh, why are you even calling? Delete it and the problem is taken care of.« Instead just be a little sensitive and encouraging to others at this point. Otherwise you will lose people quickly or they will be too fearful to call.” (male, 37 years, business unit)

In sum, information security champions through different hierarchical levels may inform others of recent information security incidents, describe that certain incidents may happen at everyone’s workstation and to every employee, and that incidents are highly likely, which in turn may increase employees’ perception that risks and threats are closer in time, more concrete, and more probable, thus evoking a greater sense of awareness. Thus, we propose:

**Proposition 5**: The presence of information security champions leads to a lower psychological distance to information security incidents.

**Potential Constraints**

During the interviews, we also disclosed that some factors may increase the psychological distance to information security incidents. One major impediment identified includes a responsibility shift, which is characterized by employees relying to a great degree on the IT department and on people in charge for taking care of information security, rather than being also personally responsible as an end-user. Upon asking interviewees if they react proactively when informed about an information security incident or if they feel determined and involved to bring informational input, a considerable amount of passivity was identified. Employees expressed high expectations that the company itself is up to date with public security news, keeps up with environmental changes, and is able to resist current threats, rather than having personal responsibility themselves.

Several employees that were considered to have a low psychological distance to information security incidents (e.g., through being personally involved) failed to recognize that the end-user is also responsible for ensuring information security. One interviewee illustrated this imbalance as follows.

“What is most important to me is that my workstation is always fully able to work. It happened to me that I opened an email that potentially, I do not know, was infected with malware. I immediately called our user support and the computer was replaced. This is the most important thing, that the IT provides a workable or let me say uncontaminated workstation.” (male, 48 years old, business unit)

Employees’ trust in a secure working environment may be one potential reason why they neglect to think about potentially negative consequences for information security.

“What comes to my working space is safe. I will just open it. And if there are the correct keywords included, then that’s it. Then we always quickly get a new PC.” (female, 52 years old, business unit)

In shifting the responsibility of information security to others, such as the IT department, employees may perceive incidents to never happen, at another company, to another employee, and are skeptical about the possibility of them happening, which in turn may result in a failure to develop a sense of self-risk, being less careful or on alert, for instance, while handling emails, and thus exhibiting a lower sense of awareness. Thus we propose:

**Proposition 6**: Employees’ responsibility shift to the IT department leads to a higher psychological distance to information security incidents.

The derived relationships between psychological distance to information security incidents and information security awareness and the effects of facilitating conditions as well as potential obstacles at an individual level of analysis are summarized in Figure 1.
Discussion

To uncover the effect of psychological distance to information security incidents on information security awareness we used a case study research design and conducted interviews among employees from different hierarchical levels of IT and business units of a multinational financial institution that was affected by an information security incident, in terms of the Locky ransomware, just two weeks prior to the investigation. Thereby we focused on the psychological distance to this information security incident and its influence on employees’ ISA. CLT was used as the underlying theoretical framework for case analysis. The results underscore the influential nature of psychological distance to information security incidents on ISA. From this point, we can conclude that when employees perceive information security incidents to occur sooner rather than later, at one’s own workstation or department rather than at another company, to oneself or employees with similar characteristics rather than very different employees, and is plausible rather than implausible, they are more conscious and alert about security issues, threats, and risks in an organizational context, and thus exhibit higher levels of ISA. Additionally, we identified factors that may increase or decrease psychological distance to information security incidents. We propose that psychological distance can be reduced by the presence of information security champions, or it might also increase through a responsibility shift to the IT department or other people in charge for taking care of information security.

Theoretical and Practical Implications

From a theoretical perspective, the results of this study provide a framework from which to extend our understanding of how the experience and perception of information security incidents impacts employees' ISA. As a rising number of employees find their workplace or organization to be externally as well as internally threatened, the ability for researchers to apply proven theory to predict and model employees' ISA becomes more important. CLT has been demonstrated to provide a stable foundation from which to reason how psychological distance shapes an employee’s perspective towards information security.
Incidents. The results of this study also provide support for the extension of CLT in an information security context through the inclusion of ISA. The research at hand exactly makes such a contribution and thus sets the stage for future empirical studies. In particular, prior research has examined isolated effects of information security incidents on employees’ ISA, such as previous negative experiences with virus or spyware (Haeussinger and Kranz 2013) or perceived susceptibility to information security incidents (Ng et al. 2009), without considering how these effects might have conceptually related underpinnings. By proposing the notion of psychological distance as a way to link these effects through a common mechanism, our results offer a more granular understanding of how employees mentally represent information security incidents on four different dimensions (temporal, spatial, social, and hypothetical) and how these mechanisms influence their ISA. In addition to allowing a reinterpretation of previous empirical results to information security incidents, the application of psychological distance also offers numerous starting points for the identification of future research possibilities. In the context of information security, psychological distance may also experience an extension by identifying further dimensions of distance and specifying their interaction. This study could be extended by using the findings of our case to empirically test the framework and propositions in a quantitative survey.

In addition to our finding that previous negative experience with an information security incident positively impacts employees’ awareness being consistent with prior research (Haeussinger and Kranz 2013), our core contribution is the insight that the degree of psychological distance, i.e. whether employees experience it as proximal or distant along four dimensions, is an important factor for employees’ ISA. As psychological distance matters, there will be some kind of threshold for the effect of prior experiences with security incidents on an employee’s ISA. Thus, the question arises how organizations are then able to achieve their ultimate goal of an organization-wide awareness of security-related threats. If some employees are only partially aware or even unaware due to their psychological distance, then an organization-wide spread of ISA is impossible. In order to achieve complete penetration of ISA, other factors potentially influencing the relationship between psychological distance and ISA may need to be considered. As employees are all part of a social network through which they exchange information, for example on information security incidents, their position in the organization may grant them some advantages or disadvantages (Burt 1982). By drawing from research on structural holes, one factor that may be considered in further studies is the degree to which employees mediate information on incidents between distinct groups (e.g., IT and business unit) in order to spread ISA in an organization (Burt 1982). As two factors – information security championing and responsibility shift to others – may influence psychological distance, they both need to come under scrutiny in subsequent research. While we know from research on organizational behavior (Bass 1990) that inspiring leaders, such as information security champions, can help to increase employees’ awareness on organizational issues it could be of great interest to study their profile by examining their traits and further individual differences compared to our leading people in organizations. Throughout our case study, we uncovered that employees have a high psychological distance to information security incidents, if they shift the responsibility to the IT department or other people in charge for taking care of information security. Research on why employees are less committed to organizational objectives such as being compliant to information security policies, is still scarce but our finding might be a first step toward explaining the consequences of employees’ responsibility shift. Within the information security field, the concept of optimistic bias is closely related to this behavior (Rhee et al. 2005, 2012), thus future research could help to uncover employees’ responsibility shift by taking the theoretical lens of individuals’ optimistic bias (Weinstein 1980).

From a practical perspective, this research acknowledges that a lack of ISA is a serious problem and causes a high potential risk for many companies as ISA is generally the first step in changing employees’ security-related behaviors (Bulgurcu et al. 2010; D’Arcy et al. 2009; Dinev and Hu 2007). The results highlight key actions that practitioners can take to influence ISA. Distance-related factors could be used to manipulate the concreteness of an information security communication (e.g., intranet articles, emails, or other security warning messages sent by the organization) thereby influencing employees’ ISA. Mimicking distance effects of time (by describing certain incidents as happening ‘every day’), space (by describing certain incidents as happening ‘at everyone’s workstation’), social (by describing certain incidents as happening to ‘you and your peers’), and hypothetical (by describing certain incidents as being ‘highly likely’) should increase employees’ perception that risks and threats are closer in time, more concrete, and more probable, thus evoking a greater sense of awareness. An important aspect in this regard is moving gradually from more central, goal-related features of information security communication (‘whether’
incidents occur) to peripheral, specific features ('how' incidents occur) in order to evoke a change from abstract to concrete mental representations of incidents. Thus, practical details of specific information security incidents could be included in security communication. Their purpose is to explain feasibility, i.e. the means to reach a secure end state (e.g., how incidents can be detected and avoided).

Our results also highlight the potential of recreating and conducting artificial information security incidents, such as feigned spear phishing attacks to decrease employees' psychological distance towards such events and thereby increasing their levels of ISA. In particular, such incidents should be conducted regularly (like an annual fire alarm test) and at everyone’s workstation to keep both temporal and spatial distance low, and to ensure the continuous attention of all employees. They should also be tailored to employees with similar job positions to decrease social distance so that employees get the experience that they personally or similar others could be affected by it. Finally, as many employees may perceive that incidents are unlikely, hypothetical distance should also decrease when they actually experience one.

Information security champions, who voluntarily take extraordinary interest in information security and who could serve as mediators of information security, should be identified and encouraged to spread security-related information among others. During weekly or monthly group meetings, for example, champions could be allotted a few minutes extra on the agenda to briefly address current information security incidents. This kind of experience sharing could be top-down or bottom-up. Leaders could share, transparently, prior information security incidents and explain direct consequences, at the same time sensitizing the employees. Conversely, employees could share their own experiences with others. The latter approach would require that experience sharing is visibly encouraged and having a failure-tolerant culture with empathetic leaders.

To counter a responsibility shift to others, organizations with a central IT help desk should evaluate in how far their employees should rely on others to solve their security-related problems. Instead of providing a final solution of the problem without describing the processes leading to it, the IT help desk could help employees to help themselves by guiding employees through the necessary steps. As illustration, an open internal handling and processing of current information security incidents could involve describing how employees have become (or could become) victims of a ransomware or similar attack. It is through the identification of the dangers and consequences of one’s own actions, an explanation of the damage caused (or that could have been caused) and possible countermeasures to avoid future incidents, that an understanding of one’s own responsibility can be created or strengthened.

Limitations and Further Research

When interpreting the results of our study, some limitations that point to further research opportunities need to be considered. The fact that the case study is based on a single organization from a certain sector, the financial sector, which is a highly information intensive environment, should be considered when attempting to generalize the findings. To extent the findings of our case study, comparative case studies could be conducted with the objective to collect richer insights and to gain a profound understanding of how employees perceive and experience information security incidents in different organizations in multiple industries.

The process of identifying the four distance dimensions (temporal, spatial, social, and hypothetical) in our interview data was to a large extent interpretive. Even though we tried to prevent subjectivity while reviewing and coding data, there is still a risk that some of our own biases might have influenced the process. We were conscious about that risk and thereby expect that identifying and evaluating the four distance dimensions was not much influenced by our personal preconceptions. Nevertheless, as our research model is based on qualitative findings, further research endeavors should quantitatively test the validity of the propositions that emerged from the exploratory study (Mingers 2001).

Another interesting research avenue is to consider how ISA spreads in organizations. In analyzing the interviews, we found that some employees, both from IT and business units, considered themselves to be a multiplier of information security in their department. Similarly, employees reported on different information channels, through which they became aware of information security issues like the Locky ransomware incident such as personal talks with the parties affected, office grapevine, remarks from their supervisors, and/or security warnings sent by the IT unit. From a social networking perspective, if organizations, for instance, try to conduct artificial information security incidents as proposed in the
previous subsection, they need to know how many employees really need to be personally reached to create an organization-wide awareness that is spread through the employees’ social network. In this regard, conducting a longitudinal study would be also beneficial to study how awareness spreads within organizations and whether the effect of information security awareness is stable over time.

References


