Trusting Security When Sharing Knowledge?

Pierre-Emmanuel Arduin, Bako Rajaonah, Káthia Marçal de Oliveira

The current reference for this work is as follows:

Arduin, PE., Rajaonah, B., and de Oliveira, K.M. (2020) Trusting Security When Sharing Knowledge?. In: Matos F., Vairinhos V., Salavisa I., Edvinsson L., Massaro M. (eds) *Knowledge, People, and Digital Transformation*. Contributions to Management Science. Springer, Cham

Feel free to email me at pierre-emmanuel.arduin@dauphine.psl.eu.

Trusting Security when Sharing Knowledge?

Pierre-Emmanuel Arduin, Bako Rajaonah, and Kathia Marçal de Oliveira

Abstract – This chapter tackles knowledge sharing by focusing on security and trust issues. Although trust is recognized as important in security issues, few studies on information systems (ISs) deal with both trust and security. Knowledge sharing relies on sense-giving and sense-reading processes which require, encourage, and even create trust within individuals. We argue that individuals are processors of information; they interpret information to create their own tacit knowledge.

Recent security reports from organizations have presented that the majority of ISs security threats involve employees within the organizations. Individuals, as well as computers, may be attacked through social engineering techniques in order to gain their trust. Despite this evidence, most of work has focused on the control of outsider security threats rather than of insider security threats, particularly when humans are perpetrators.

In this chapter, we propose to study insider threats with the factor of trust during knowledge sharing processes. Through their trust-related attitudes and behaviors, knowledge sharers may induce insider threats for security. The proposition is twofold: (1) using interviews and self-report questionnaires to collect information about trust, and (2) defining ontologies to categorize such information about trust. The proposition is then discussed at the end of this chapter, notably in terms of problems and answers leading to study trust in security when sharing knowledge.

Keywords – Knowledge sharing, tacit knowledge, trust, insider threats, security.

I- Introduction

Web-connected databases and information systems, as well as cloud-based platforms have become so indispensable to enterprises and many other kinds of organization to support knowledge sharing that managing security issues have become of a priority. Indeed, the security of Web-based systems is a worldwide challenge due to the seriousness of the consequences of security breaches. The media relates almost every day security issues of Web-based systems. For instance, the BBC News app has a daily updated specific page dedicated to cybersecurity. Taking just the case of information systems (ISs), in the last years, much research and practice have focused on protecting information systems and data from unauthorized access, disclosure, modification, or destruction (Dhillon and Backhouse, 2000; Whitman and Mattord, 2011). The main idea has been to avoid the access of non-authorized people/software systems that could generate any kind of damage.

Nevertheless, security reports from industry (PwC, 2018; Kaspersky, 2015; Keeney et al., 2005) show that, contrary to the complex infiltration procedures, the security problems were caused by hacking a specific IS component: the individuals, several times own employees of the organization. Loch et al. had raised this kind of IS security threat in 1992, distinguishing between insider (internal) and outsider (external) threats, that come from human or natural actions which, in turn, can be accidental and intentional (Loch et al., 1992). Individuals may be benevolent, as well as malevolent, particularly through techniques from psychological principles and social engineering (Mitnick and Simon, 2011): the attacker gains the trust of the target to persuade him/her of the truthful nature of the information that they are being sent.

Individuals are entry-points, as well as computers and digital artifacts are. Organizations have to be aware of such a special feature when considering knowledge sharing: human behavior is harder to predict and to manage than digital artifacts processing are. However, nowadays outsider security threats have been widely explored through technological solutions (e.g. cryptography, firewalls) and far less investment is made to control insider threats (Collwill, 2009). This chapter proposes to deal with knowledge sharing by focusing on trust and security, which is in an increasingly common context in the Web-based society.

Working in this direction involves putting face-to-face technology (analysing the issues of IS security) and human (as both a user of the IS and a potential attacker against another human via an IS). Dealing with these issues together is innovative and challenging, requiring truly multidisciplinary work that takes social, technological, and management aspects into account. We argue that the individual is a carrier of knowledge and a processor of information. He/she is a component of the Enterprise's Information and Knowledge System (Arduin et al., 2015). Thus, ISs carry information as a source of knowledge. Only individuals can possess genuine knowledge, resulting from their interpretation of information (Tsuchiya, 1993). Therefore, individuals' thought processes have to be considered when managing ISs' security (Willison and Warkentin, 2013).

As mentioned earlier, we propose to tackle this security issue by considering trust. Section II presents the theoretical background. The concept of knowledge sharing is first explained, then the particular problem of insider threats is considered, which is followed by an explanation of that problem through the trust factor. Section III proposes to investigate the plausibility of this explanation with regard to the security of knowledge sharing, particularly by considering insider threats. Interviews and self-report questionnaires are presented as techniques to collect information about perceived trust, whereas ontologies are exposed as a technique to categorize such information about trust. A discussion on identified risks and answers concludes this section. The study presented in this chapter leads to understand ways of trusting security when sharing knowledge.

II- Theoretical background

The theoretical background aims at describing the main concepts considered in this chapter. The unifying thread is the relationships between the knowledge sharers, insider threats they may represent

for security and their trust. The Section details first the concept of knowledge sharing. The issue of insider threats is then explained. Last, an explanation in terms of trust is proposed.

1. Knowledge Sharing

Polanyi (1967) was interested in the way in which we endow our discourse with meaning (by speaking or by writing, for example) and in what we attribute meaning to (by listening or by reading, for example). Although they are informal, these actions possess a characteristic model that he calls the structure of tacit knowing: "Both the way we endow our own utterances with meaning and our attribution of meaning to the utterances of others are acts of tacit knowing. They represent sense-giving and sense-reading within the structure of tacit knowing" (Polanyi, 1967, p. 301).

Here is a good example on the way Polanyi highlighted knowledge sharing, and particularly tacit knowledge sharing: One morning he saw his son come in, and wanted to pass a letter on to him. Remembering that his son only spoke English, he checked the letter and realized that it was in a foreign language. Polanyi was therefore conscious of the meaning conveyed by the letter but not the words that had conveyed it. He then explained the contents of the letter to his son in English. This clearly shows that one can (1) possess the meaning of a text without knowing the text itself and (2) put this inarticulate meaning into words. We can therefore possess unarticulated knowledge that Polanyi calls tacit knowledge. Polanyi has insisted since 1967 on the fact that: "[…] modern positivism has tried to ignore it, on the grounds that tacit knowledge was not accessible to objective observation" (Polanyi, 1967, p. 306). As a temporary difficulty, the fact that the language is nothing until there is knowledge of its meaning was ignored at the time and that still seems to be the case today. There has been extremely large economic investment in information technology and collaborative tools has been since the 1970s. Yet, as Landauer (1995) remarked, the productivity of the services who invested in stagnated throughout the world.

The retranscription of the letter that Polanyi offered his son was that of the meaning of the letter as he understood it. Imagine that the letter describes a scene that the sender, a traveler, witnessed while he wrote it. Maybe he admired a landscape, a particular instance of trees, fields, rivers and mountains. When he reported on the scene, he used the general terms "trees", "fields", "rivers" and "mountains", which do not transmit the particular instance that he has witnessed. In doing so, by choosing the words to describe his experience, he has performed a sense-giving process (Fig. 1), he has endowed them with meaning for himself. His lived experience, his perceptions and his tacit knowledge of the place visited have thus been communicated in the form of made explicit knowledge, a letter, whose meaning was tacit.

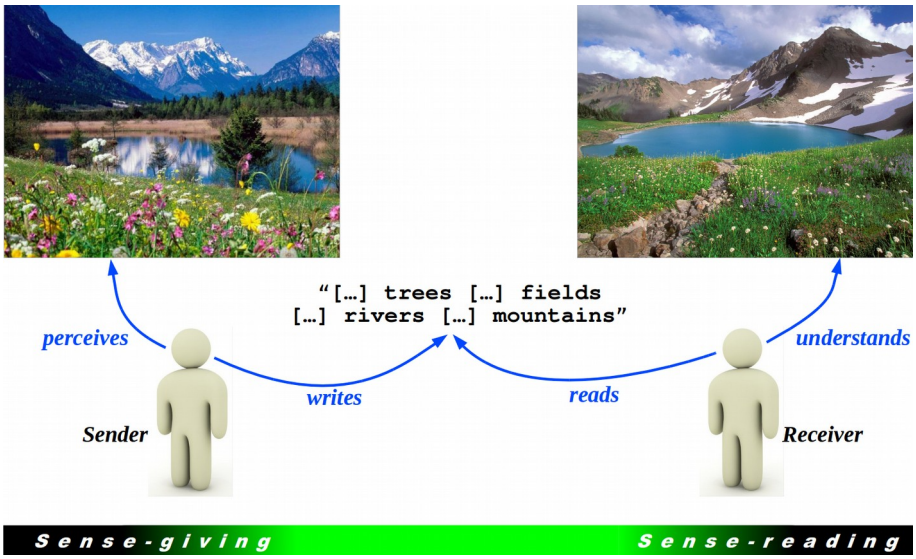

Fig. 1 – Tacit knowledge sharing: from sense-giving to sense-reading (Arduin, 2018)

In receiving the letter and reading it, Polanyi perceives shapes and colors, from which he understands words. Once perceived, the words are forgotten to give way to the meaning attributed to them, which corresponds to a sense-reading process (Fig. 1). He is therefore conscious of the meaning of the letter without remembering the text. That is the reason why he forgot that his son, who only spoke English, could not read it.

By communicating his lived experience in a letter, the sender has given meaning to the words, made explicit knowledge, whose meaning is tacit: "[...] into a communication which was a piece of explicit knowledge, the meaning of which was tacit. All knowledge falls into one of these two classes: it is either tacit or rooted in tacit knowledge" (Polanyi, 1967, p. 314). In this way, all knowledge is either tacit or rooted in tacit knowledge.

Polanyi insists heavily on the "contradiction" of the existence of made explicit knowledge, since, without their tacit coefficients, all words, all formulas, all maps and all images are simply devoid of meaning. The example that he uses is that of the cyclist who at any time is offsetting his imbalance, by turning the bicycle in a curve with a radius proportional to the square root of its speed divided by the angle of his imbalance. This rule, although made explicit, is useless in learning how to ride a bicycle. Moreover, for someone who does not grasp its tacit meaning, it remains not understood.

However, knowledge sharing raises issues of security, particularly issues of insider threats as individuals are involved as knowledge holders.

2. Insider threats and security

The main concepts behind IS security are protection of both information and technology against unauthorized access and/or modification (e.g. Dilhon and Backhouse, 2000; Whitman and Mattord, 2011). The problem is therefore to design secure IS, in other words, to design systems such as their users could expect both information and technology to be preserved from unauthorized access and modification. From the perspective of users, IS security is thus a matter of IS trustworthiness: the user's perceptions of IS would influence his/her expectations that his/her data could not be accessed and/or modified by a third other than him/her and authorized people of IS. This is particularly crucial in the case of knowledge sharing, where trust is a common denominator to initiate and perpetuate knowledge sharing processes.

At the beginning of the 1990s, the literature on information systems security had already affirmed that there was "a gap between the use of modern technology and the understanding of the security implications inherent in its use" (Loch et al., 1992, p. 173). The massive arrival of microcomputers was also accompanied by questions regarding the security of interconnected systems where computer science was previously mainframe oriented.

Indeed, the number of technological artefacts has exploded and this increase has gone hand in hand with the evolution of their various uses (Canohoto et al., 2015). Yesterday, a terminal connected the user to the computer, while today entry points into the information system are multiple, universal, interconnected and increasingly discreet. Employee's social activity can be supported by social networks and their health maintained using connected watches.

The taxonomy of threats targeting the security of information systems proposed by Loch et al. (1992) presented in Figure 2 is disturbingly topical, with regard to the four dimensions that make up his angle of analysis: (1) sources, (2) perpetrators, (3) intent, and (4) consequences. It should be recognized that independent of the sources, perpetrators, and intent of an attack, the consequences remain the same: disclosure (of profitable information), modification or destruction (of crucial information), or denial of service (by hindering access to resources). These consequences are covered in the 2013 ISO/IEC 27001 standard: information security management, which defines information security management systems as ensuring the (1) confidentiality, (2) integrity and (3) availability of information (ISO/IEC, 2013).

A business's firewall constitutes a protection against external threats, which appear on the left branch in Figure 2. Authors such as Willison and Warkentin (2013) represent a part of the literature on information systems security that tends to pay attention to insider threats, more particularly those whose perpetrators are humans with the intention to cause harm (upper right branch in Figure 2).

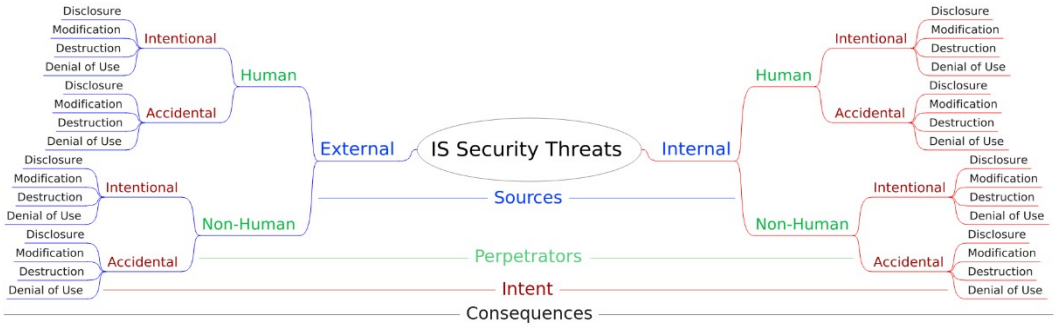

Fig. 2 – Taxonomy of IS security threats (inspired from Loch et al., 1992)

For authors such as Arduin (2018), insider threats may be categorized along two dimensions: (1) whether the character of the threat is intentional or not, and (2) whether its character is malicious or not. From the point of view of the employee, who may constitute the entry point into the system, an insider threat can be:

1. unintentional: wrong actions taken by an inexperienced or negligent employee, or one manipulated by an attacker; for example, an inattentive click, input error, accidental deletion of sensitive data, etc. (Stanton et al., 2005);
2. intentional and non-malicious: deliberate actions by an employee who derives a benefit but has no desire to cause harm; for example, deferring backups, choosing a weak password, leaving the door open during a sensitive discussion, etc. (Guo et al., 2011);
3. intentional and malicious: deliberate actions by an employee with a desire to cause harm; for example, divulging sensitive data, introducing malicious software into the computer system, etc. (Shropshire, 2009).

The study presented in this article focuses on the manipulation and social engineering techniques that exploit unintentional insider threats (category 1 above). Even though the attacker is outside the system and the organization, he makes an employee, a component of the system, unintentionally facilitate his/her infiltration: the latter has, for example, clicked on a link or even opened the door to a self-proclaimed delivery person with a self-proclaimed task. A social engineer is an attacker who targets a legitimate user from whom he/she obtains a direct (rights of access, harmful link visited, etc.) or indirect (vital information, relationship of trust, etc.) means to get into the system (Mitnick and Simon, 2011).

As new technological solutions are developed, the exploitation of hardware or software weaknesses becomes more and more difficult. Attackers are then turning toward another component of the system susceptible to attack: the human one. For authors as Schneier (2000): "Security is a process, not a product". For others such as Mitnick and Simon (2003, p. 14), breaching the human firewall is "easy", requiring no investment, except for occasional telephone calls and involves minimum risk. Every legitimate user constitutes thus an unintentional insider threat to the information system's security.

Individuals are not trained to be suspicious of others. Consequently, they constitute a strongest threat to the security of the information system insofar as any well-prepared individual can win their trust.

3. The question of trust with regard to security

As mentioned earlier, few studies on information systems deal with both trust and security despite the fact that trust is recognized as important in security issues. Trust helps reducing the perceived complexity of social systems (Luhmann, 2000; Möllering, 2001). It does exist in situations of uncertainty and, consequently, of risk: a trusting agent is a risk-acceptant agent (Castelfranchi and Falcone, 2000). The mechanism of trust is to mentally reduce the occurrence of possible futures (Lewis and Weigert, 2012), which provides an illusion of control to the trusting agent and results in a psychological state of expectations (Castelfranchi and Falcone, 2000). Trust is a three-part relationship including the trusting agent, the object of trust (i.e., the trusted), and the expectations that relate the trusting agent to the trusted party (Hardin, 2001): in a word, A (trusting-agent) trusts B (trusted party) to do X (what is expected).

The object of trust can be an individual, a group of individuals, an organization, an institution, or a technology. Whatever the object of trust, trust is an intermediate factor that may guide our attitudes and decision-making processes with regard to this object (Kramer, 1999; Lee and See, 2004). For instance, the decision to rely or not rely on a technology may be guided by one's level of trust in the technology. Depending on the context reliance on people, organization, technologies, etc. might be appropriate, but it might be also not appropriate: it is the concept of trust calibration described by Muir (1987) who is one of the firsts who studied trust in machines.

Trust calibration requires the understanding of the context and of how much the trusted-parties will be able to fulfil or not fulfil what is expected from them in that context, that is, how much they could be trusted or distrusted. Experimental studies have shown that trust could be considered as a continuous variable opposing trust and distrust (e.g, Jian et al. 2000). The level of trust (or distrust) would depend on the trusting agent's goals, beliefs, and assessments, which constitute the dimensions of trust, or what makes trust level changing (e.g., Hoffman et al., 2013). These dimensions, viewed from the perspective of the trusting-agents are their "good reasons" to trust or distrust (Möllering, 2001).

As for the context of this chapter, that is to say, considering ISs in the context of knowledge sharing, trusting agents and trusted parties are multiple and various, and the same is thus true regarding expectations (Figure 3).

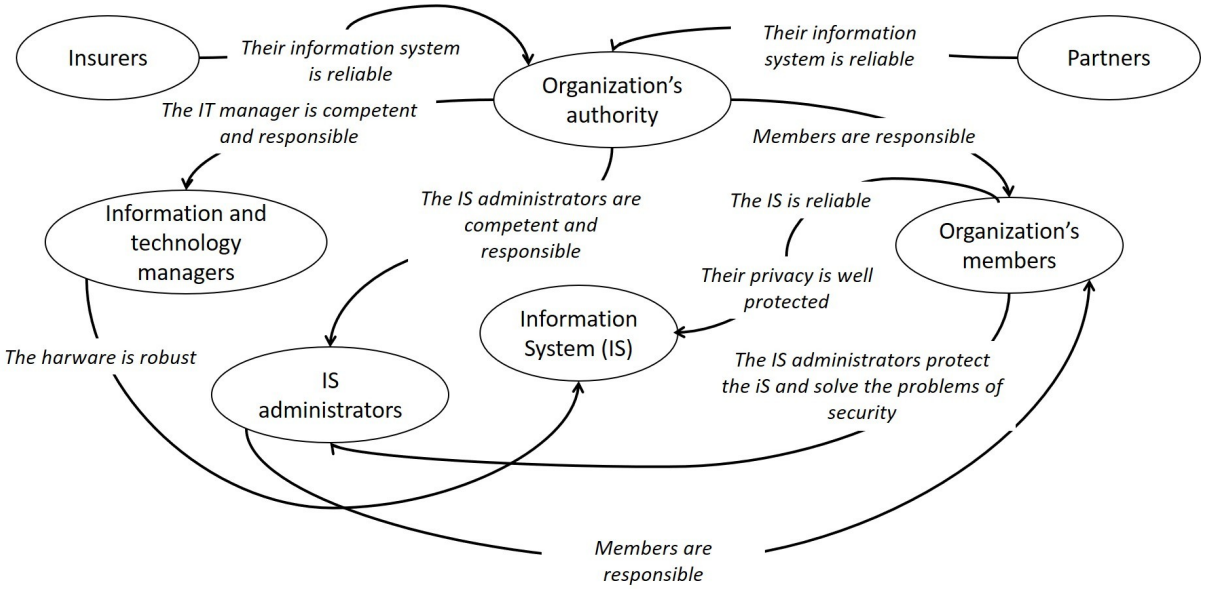

Fig. 3 – The multiplicity of trusting-agents, trusted parties, and expectations with regard to an organization's information system (adapted from Rajaonah, 2017, p. 117).

Taking the example of an organization which activities go through an IS, Figure 2 shows that each part of the organization is responsible for IS security and has good reasons to be confident, at different

levels. Let us focus on the organization's members who interest us as potential insider threats: they are expected to behave in a responsible way by both the organization's managers and the IS administrators. In return, the members have expectations toward the information system and their administrators. In a word, they trust both the IS and their administrators. In fact, they also trust the other organization's members, themselves and, perhaps, the attackers, at least they may believe the attackers would spare them (but not the others), who knows!

The main hypothesis could therefore be that users of ISs may be intentionally harmful because their trust in technology, people, and themselves is not well calibrated, as well as, corollary, they are too much optimistic.

Let us review some results in the field of psychology which could justify that hypothesis.

a. Optimism. People tend to be naturally toward optimistic, which is namely the bias of unrealistic optimism: Weinstein (1980) shows that people tend to believe that positive events are more likely to happen to them than to others, and that negative events are less likely to happen to them than to others. That is true in situation of risk in which people tend to believe that they are less exposed to risk than others are, which has consequences on their decisions and behaviors (e.g., Lench and Bench, 2012; Slovic et al., 1984). It can be thus supposed that their optimism leads them to be excessively trustful with regard to security, which includes attackers: in their natural optimism, individuals may fail to consider that they could be a target for attackers.

b. Lack of awareness and knowledge. Optimistic bias could be partly explained by lack of awareness and/or knowledge about objective risks. Sasse and Flechais (2015) notice that organizations' members tend to lack of understanding of information security issues and of how their behaviors could be a threat against security. As shown in the EY's Global Information Security Survey 2015 (EY, 2015), employees are often careless and unaware about cybersecurity. It is thus a fact that those people are not aware that they are potentially harmful to the organization's information security. It can be then assumed that the lack of awareness and knowledge contributes to induce excessive optimism and trust with regard to security.

c. Self-confidence and illusion of control. The illusion of control had been described in the seventies as being "an expectancy of a personal success probability inappropriately higher than the objective probability would warrant" (Langer, 1975, p. 311). More simply, the illusion of control is the tendency to believe that we have the ability to control events (who has never blown on the dice before throwing them?). Self-efficacy is a closely related concept: perceived self-efficacy is the people's beliefs in their efficacy to influence events that affect their lives (Bandura, 1997). There is therefore a tendency for people to be naturally confident in their own abilities to master the situation. Despite their lack of awareness and knowledge, it can be assumed that organizations' members are over-confident in their skills to deal with information security, and that may be also true concerning that personal data (Akhter, 2014). It can also be assumed that their over-confidence leads them to minimize security issues, or even believe that attackers could not reach them.

d. Responsibility. Organizations' employees tend to believe that security is the matter of the others (see Hadlington, 2018). In other words, they do not consider cybersecurity as a shared issue. It can thus be assumed that they prefer being excessively trustful towards organizations' authorities and IS's administrators than questioning their own attitudes and behaviors.

Optimistic bias, lack of awareness and knowledge, illusion of control, and misplaced responsibility could be good reasons for ISs users to be excessively trustful regarding security and then constitute insider threats. We propose an approach that would categorize these users through an analysis of *their* good reasons.

III- Proposition: studying insider threats with the factor of trust

The objective of this section is to propose to investigate the plausibility of explaining insider threats with the factor of trust. This proposition consists in (1) collecting information about trust, attitudes and behaviors of knowledge sharers, and (2) categorizing this information into meaningful units that could be related to different levels of insider threats. The section begins with the techniques of interview and questionnaire used in social sciences, and then explains the technique of ontology used in computer sciences.

1. Interviews and self-report questionnaires to collect information about trust

We propose to start by gathering information from the three-part circle of ISs security from the perspective of the users' trust, namely, the organization' authority, the IS administrators, and the simple users (not experts). The techniques used will be interviews and self-report questionnaires.

Interviews are used to collect focused and qualitative data and are particularly relevant to obtain information about participants' experiences and viewpoints (Turner, 2010). This author distinguishes (a) the informal conversational interviews which lack of structure allows interviews to be flexible, (b) the general interview guide approach in which questions may be adapted to the respondents during the interview in order to collect the desired information, and (c) the standardized open-ended interviews that focus the answers on specific questions.

As for self-report questionnaires, they could be used to gather both qualitative and quantitative data. They are perfect to gather opinions and measure attitudes (see Grawitz, 1993). The main advantage of closed questionnaires is that they are economic in the sense that the same questionnaire can be completed by thousands of people. Open questions allow to collect in-depth answers because answers are not constrained, but their analysis is rather complex because of the heterogeneity of the collected information. Closed questions structure the answers with pre-set responses, which facilitate data analysis, especially when there are hundreds or thousands of participants. Another advantage of closed questions is that they can provide quantitative information through ordinal data.

We propose to use standardized open-ended interviews and self-report questionnaires based on closed-questions. The techniques used depend on the kind of information which we desire, and thus on the targeted respondents in one or more organization(s). The participation of end-users of an organization's information system is therefore the main pre-requisite.

Interviews, the first step, are used to collect information from authorities and administrators in the form of face-to-face open-ended interviews focused on the organization members' attitudes and behaviors concerning information security from the experience and viewpoints of authorities and administrators. The interviews could be carried out individually or with a staff of more than one individual (it is then similar to a focus group). Preliminary questions that would be the same for each respondent would be prepared, but the responses will be open to not constrain the respondents. The main questions will be related to the basic rules that are communicated to the users and the means of communication; the users' self-reported behaviors and underlying attitudes; their trust in the users; their categorization of the users, as well as the different levels of the user's harmfulness; etc. The data analysis will be performed by at least two researchers to avoid biases of interpretation. The results will be used to build the questionnaire survey dedicated to the users.

The next step (self-report questionnaires) aims to collect information from the organization' non expert members (i.e., neither technicians nor engineers working on the organization's IS) in the form of a closed questionnaire survey. Apart from the demographics, each question will be evaluated using the visual analogical scale (VAS) in order to get both qualitative and quantitative information. For example, see Muir and Moray (1996) who used 100-mm scales to measure self-reported trust in automated systems. The VAS relies on the premise that, in our case, the variables investigated through

the questionnaire's items are continuous variables, which is the case for attitudes that can thus be directly measured. Consequently, the use of such a scale will enable to carry out correlation analysis in order to relate users' level of trust to the strength of their good reasons to trust or distrust, as well as to carry out statistical inference analyses if necessary. Even though, the questionnaire will be built according to the information collected at the previous step, the items will necessarily investigate the users' opinions, attitudes and behaviors toward information security and data privacy, as well as their related level of self-confidence, their perceptions of cyber-risk, their awareness and knowledge about cybersecurity, etc. A clustering analysis will be carried out complementary to the correlation analysis in order to provide information for the development of the ontology that takes the categorization of the users accordingly to their degree of harmfulness into account.

2. Ontologies to categorize information about trust

Ontology is a description of entities and their properties, relationships, and constraints expressed via axioms (Gruninger and Fox, 1995). Domain ontologies (Guarino, 1998) express conceptualizations that are specific for a particular domain (e.g., transportation, family organization, risks management). They put constraints on the structure and contents of domain knowledge. For instance, when talking about family, one can say that a child must have at least a parent.

Ontologies may serve to various purposes in the context of knowledge management (Anquetil et al., 2007):

- Reference on a domain - made explicit knowledge serves as a reference to which people, looking for detailed information on the domain modeled, may use;
- Classification framework - the concepts made explicit in an ontology are a good way to categorize information on the domain modeled. Indication of synonyms in the ontology helps avoiding duplicate classification. Other relations among the concepts of the ontology help one browsing it and finding an information one is looking for;
- Interlingua - tools and/or experts wishing to share information on the domain modeled, may use the ontology as a common base to resolve differing terminologies.

Several works on ontology about security and trust can be found in literature. We quote, for instance the proposition of Viljanen (2005), Huang and Fox (2006), and Fenz and Ekelhart (2009).

Viljanen (2005) analyzed thirteen trust models to identify the main features about trust considered in which one of them. As result they assumed that the union of these features across all models provides a list of trust input factors. These factors were in turn organized in an initial ontology. This initial ontology considers only concepts, no axiom was defined.

Huang and Fox (2006) also defined an ontology, but focused on transitivity issuers. They discuss that the use of web application implies the need of trust between entities (sometimes unfamiliar or unknown) that interacts with each other. They argument that social-networks have been proposed as a remedy to assure trust in the web, however, as consequence trust need to be transitive. They proposed, therefore, a formal ontology that explicit the semantics for trust transitivity.

Fenz and Ekelhart (2009) have proposed a large ontology that organize the knowledge about information security. Their goal is to support and enhance risk management approaches. To that end they reuse some known taxonomies in the domain of security and telecommunication.

All these works deal with the concepts of trust and security separately in ontology models. Developing an ontologyusing Protégé[1], for example, relies on basic steps that are described below from Noy and McGuiness (2010):

[1] https://protege.stanford.edu

a) Determining the domain and scope of the ontology through basic questions is first required:

1. What is the domain covered by the ontology? A domain is the representation of a part of the reality. Here, the objective is to represent the role of organizational members' trust in IS's security threats. The domain will thus cover IS security and individual's trust in organizations.
2. What is the use the ontology? The ontology will allow the researchers to categorize the users of an organization's IS in terms of their potentiality to be insider threats; the ontology will be thus useful to the IS's administrators, technicians, and engineers to design countermeasures and develop targeted information to the organization's members.
3. For what questions the information in the ontology should provide answers? These questions could be about the good reasons of organizations' member to trust or distrust their organization's IS, other Internet-connected systems, their colleagues, and the IS's managers, but also about their perceptions of cyber-risk; their level of awareness, knowledge, and practice, as well as their level of self-confidence, concerning their skills regarding cybersecurity.
4. What are the competency questions, that is that the ontology should be able to answer? The competency questions will be defined from the answers to the interviews and self-report questionnaires. Nevertheless, the ontology should be able to provide information about the relevant dimensions of the trust of IS's users in terms of cybersecurity, as well as the relationships between these dimensions and the potentiality of the users to be insider threats.

b) Considering reusing other ontologies could be useful: A state-of-the-art of existing ontologies related to the domains of cybersecurity (e.g., Oltramari et al., 2015) and of trust (e.g., Viljanen, 2015) will be necessarily carried out, even before defining the competency questions in order to make sure that the proposed ontology will be useful for the purpose and/or even enrich the existing ones.

c) Defining the important terms of the ontology, as well as the related concepts: This needs expert knowledge about knowledge sharing, information system, trust, and psychology (considering that being or not being trustful is a matter of cognitive and social psychology). The terms and related concept should be cover those of the questions defined in the first step, as well as of their expected responses.

d) Defining classes (or concepts) and arranging them in a taxonomic hierarchy: The objective of the ontology is to categorize organization's users in order to provide appropriate information and countermeasures to potential insider threats. We can rely on the bottom-up development process described in Noy and McGuinness (2010) by starting from the results of the analyses of correlation and clustering, that is to say from the categories of users related to the degrees of their harmfulness to finish at the level of the most general concepts.

e) The next steps before developing the ontology are to define the properties of classes and sets of properties (slots), as well as values of the properties. Such properties may be defined from the clusters obtained during the previous step.

Doing so, developing an ontology creates knowledge. In our case, trust, insider threats and security will contribute to the ontology. Information about trust collected through interviews and self-report questionnaires will answer and refine the competency questions raised during ontology definition. Some success indicators are the number of respondents who will accept to be interviewed and the number of respondents in the survey. Such indicators, as well as identified risks are now discussed.

3. Discussion

Although it seems obvious that trust and security are two concepts that are intrinsically associated, since the trust that a user has in a system depends, among other factors, on the security that it provides, explicitly associating these concepts is not trivial and very challenging. It requires an analysis from different points of view (social, psychological, managerial and technical), implying a multidisciplinary team. It is also challenging to define an ontological model that represents the theory on the subject but also the contexts and intents of knowledge sharers. Focusing the study on insider threats leads to deal with probably untapped issues in the case of knowledge sharing.

Nevertheless, based on our goals and on the chosen method, we identify the following problems that may occur to carry out the investigation study:

a) Conflict relating to intellectual property, regarding access and use of research results – this risk may appear if several institutions participate to the study. To mitigate this risk, we recommend to predefine types of protection and exploitation of results that will be formally signed by all participants in an intellectual property agreement at the beginning of the project. In the case of students integrating the project, we recommend that they also be asked to sign this agreement.

b) Risk related to data collection (not secure, lost, unverified) – Interviews and self-report questionnaires to collect information about trust are planned. The results of these surveys will be used in the ontology definition. Survey data may risk of being accessed and modified, lost or unverified to assure its provenance and correctness of the collection procedures. To mitigate this risk, we recommend the use for the survey of a well-known platform from one of the partners.

c) Breach of confidentiality – This risk is related to the need of validation of the study with real cases from industry. A formal agreement of confidentiality has to be signed by industry and the consortium representatives. In this agreement it will be clearly defined what can be disclosed or not about the study carried out.

As the reader may understand, this chapter focuses not only on knowledge sharing, which already is a sensitive field of study, but also on trust, insider threats and security. We have observed within industrial fields that it is extremely hard to obtain an access to the research material needed for such a study, *i.e.* knowledge sharers accepting any interview or self-report questionnaire. We are currently experiencing ethnographic workplace study in the sense of Jordan (1996) to mitigate such a reserve from industrial partners.

Conclusion

Nowadays, hacking digital artifacts supporting ISs is more a militarist and intellectual exercise than an optimized crime. Through procedures, code fragments and infrastructures with known, managed and rational behaviors, the digital part of ISs has been secured and may now be trustworthy. Moreover, ISs also contain a human part leading us to focus on a certain category of threats that are no longer outside organizations; their firewalls being efficient, threats do no longer target digital artifacts and computers which have become too safe. In this chapter, we argued that threats may be human and inside organizations and particularly during knowledge sharing processes. In other words, we defend that the biggest threat to an organization's IS does not come from outside. It is often due to internal factors, whether intentionally or not. Organizations will be, are, and/or have already been confronted with attacks coming from their own employees, users of their information system. Attacked organizations are not always aware of having been attacked, and when they are aware of having been attacked, they do not always report it. Among these internal factors, which are unfortunately exploited by hackers to carry out attacks, one can mention the lack of awareness among knowledge sharers of certain practices. For example, to override increasingly effective security systems against external attacks, new methods of attacks based on social engineering are more and more being implemented. They use the internal staff of an organization as an attack vector. One can also mention the uncontrolled use of

access rights and privileges that are sometimes attributed in little rigorous to certain knowledge sharers who thus become potential vectors of attacks against the IS security.

These attacks use all means contributing to the functioning of the organization including e-mail, smartphones / tablets and social media. As a consequence, these attacks deal with several issues: social (e.g., interrelationship among employees and their managers), economic (e.g., financial loss), regulatory (e.g., non-respect or non-existence of adequate policies of the organization), and industrial (e.g., security of industry objectives).

In order to defend against attacks inherent to the human factor, and from the technical point of view, one needs to identify the vectors, the attack surfaces, the agents used to perpetrate these attacks and the possible internal attackers. We argue that cognitive processes, as well as organizational contexts influence the ways security may be trusted during knowledge sharing processes.

References

Akhter, S. H. (2014) Privacy concern and online transactions: The impact of Internet self-efficacy and Internet involvement. *Journal of Consumer Marketing*. 31(2), 118-125.

Anquetil, N., Oliveira, K. M., Souza, K. D. De, Dias, M. (2007). Software Maintenance Seen as a Knowledge Management Issue. Information and Software Technology, v. 49 (5), 515-529.

Arduin, P-E. (2018). Insider threats, Wiley-ISTE.

Arduin, P-E., Grundstein, M., and Rosenthal-Sabroux, C. (2015). Information and Knowledge System, Wiley-ISTE.

Bandura, A. (1997) *Perceived self-efficacy: The exercise of control*. New York, NY: W.H. Freeman/Times Books/ Henry Holt & Co.

Canohoto, A.I., Dibb, S., Simkin, L., Quinn, L, and Analogbei, M. (2015). Preparing for the future – how managers perceive, interpret and assess the impact of digital technologies for business, In: Proceedings of the 48th Hawaii International Conference on System Sciences.

Castelfranchi, C. and Falcone, R. (2000) Trust Is much more than subjective brobability: Mental components and sources of trust. In: Sprague, R. H. (ed.) *Proceedings of the 33rd Annual Hawaii International Conference on System* Sciences, 7 January 2000, Maui, HI, USA. Piscataway, NJ, IEEE.

Collwill, C. (2009) Human-factors in information security: the insider-threat – who can we trust these days?, Information Security Technical Report 14, 186-196.

Dhillon G., Backhouse J. (2000) Technical opinion: Information system security management in the new millennium, Comm. of the ACM, 43(7), 125-128.

EY (2015) *Creating trust in the digital world. Global Information Security Survey (GISS) 2015*. Available from: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf [Accessed 6th May 2019].

Fenz, S., Ekelhart, A. (2009). Formalizing Information Security Knowledge. Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 183-194.

Grawitz, M. (1993) Méthodes des sciences sociales (9° éd) [Methods in Social Sciences]. Paris: Dalloz.

Grüninger, M, Fox, M.S. (1995). Methodology for the Design and Evaluation of Ontologies, Technical Report, University of Toronto, Toronto, Canada.

Guarino, N. (ed.). (1998). Formal Ontology in Information Systems. Proceedings of FOIS'98, Trento, Italy.

Guo, K. H., Yuan, Y., Archer, N.P., and Connelly, C.E. (2011). Understanding non-malicious security violations in the workplace: a composite behavior model, Journal of Management Information Systems, 28(2), pp. 203–236.

Hadlington, L. (2018) The 'Human Factor' in cybersecurity: Exploring the accidental insider. In: McAlaney, J., Frumkin L. A., & Benson, V. (eds) *Psychological and Behavioral Examinations in Cyber Security*. Hershey, PA, IGI Global, pp. 46-63.

Hardin, R. (2001) Conceptions and explanations of trust. In: Cook, K. S (ed) *Trust in Society*. New York, Russell Sage Foundation, pp. 3-39.

Hoffman, R. R., Johnson, M., Bradshaw, J. M., & Underbrink, A. (2013). Trust in automation. *IEEE Intelligent Systems*, 28(1), 84-88.

Huang, J., Fox, M.S. (2006) An Ontology of Trust – Formal Semantics and Transitivity. ICEC,06, 259-270.

ISO/IEC (2013). ISO/IEC 27001, Information Security Management. Technical Report.

Jian, J. Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, 4(1), 53-71.

Jordan, B. (1996) The design of computer-supported cooperative work and groupware systems, chapter in *Ethnographic workplace studies and computer supported cooperative work*, 17-42, North Holland/Elsevier Science.

Kaspersky (2015) Carbanak APT – The great bank robbery, Kaspersky Lab report, February 2015 (available on: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf).

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005) Insider Threat Study: Computer Systems Sabotage in Critical Infrastructure Sectors, CERT, Software Engineering Institute, Carnegie Mellon University.

Kramer, R. M. (1999) Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, 50(1), 568-598.

Landauer, T. K. (1996). *The trouble with computers: Usefulness, usability, and productivity*. MIT press.

Langer, E. J. (1975), The Illusion of Control. *Journal of Personality and Social Psychology*, 32(2), 311-328.

Lee, J. D & See, K. A. See. (2004), Trust in Automation: Designing for Appropriate Reliance. *Human Factors* 46(1), 50-80.

Lench, H. C. & Bench, S. W. (2012) Automatic Optimism: Why People Assume their Futures will be Bright. *Social and Personality Psychology Compass*, 6(4), 347-360.

Lewis, J. D. & Weigert, A. J. (2012). The Social Dynamics of Trust: Theoretical and Empirical Research, 1985-2012. *Social Forces* 91(1), 25-31.

Loch, K., Carr, H., Warkentin, M. (1992) Threats to Information Systems: Today's Reality, Yesterday's understanding, MIS Quaterly, 16(2), 173-186.

Luhmann, N. (2000) Familiarity, Confidence, Trust: Problems and Alternatives. In Gambetta, D. (ed) *Trust: Making and Breaking Cooperative Relations*. Department of Sociology, University of Oxford, pp. 94-107. Available from: http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf [Accessed 6th May 2019].

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Möllering, G. (2001) The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension. *Sociology* 35(2), 403-420.

Muir, B. M. (1987) Trust between Humans and Machines, and the Design of Decision Aids. *International Journal of Man-Machine Studies*, 27(5-6), 527-539.

Muir, B. M. and Moray, N. (1996) Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics*, 39(3), 429-460.

Noy, N. F. & McGuinness, D. L. (2010) *Ontology Development 101: A Guide to Creating your First Ontology*. Stanford University Stanford, CA. Available from: https://protege.stanford.edu/publications/ontology_development/ontology101.pdf [Accessed 6th May 2019].

Oltramari, A, Henshel, D., Cains, M., & Hoffman, B. (2015) Towards a Human Factors Ontology for Cyber Security". In: *Proceedings of Tenth International Conference on Semantic Technology for*

Intelligence, Defense, and Security, 18-20 November 2015, Fairfax, VA, USA, pp. 26-33. Available from: http://ceur-ws.org/Vol-1523/STIDS_2015_T04_Oltramari_etal.pdf [Accessed 6th May 2019].

Polanyi, M. (1967). Sense-giving and sense-reading. *Philosophy*, *42*(162), 301-325.

PwC (2018) The Global State of Information Security® Survey 2018 - Strengthening digital society against cyber shocks, PriceWaterhouseCoopers report.

Rajaonah, B. (2017) A View of Trust and Information System Security under the Perspective of Critical Infrastructure Protection. *Ingénierie des Systèmes d'Information*, 22(1), 109-133.

Sasse, M. A. & Flechais, I. (2005) Usable Security: Why Do We Need It? How Do We Get It? In: Lorrie Cranor L. & Garfinkel, S (eds) *Security and Usability: Designing Secure Systems that People Can Use*,. Sebastopol, CA: O'ReillyMedia, pp. 13-30.

Schneier, B. (2000). "The process of security." Information Security 3 (4), 32.

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. Information Management & Computer Security, Vol. 17 Iss 4 pp. 296 - 310.

Slovic, P, Fischhoff, B., & Lichtenstein, S. (1984) Behavioral Decision Theory Perspectives on Risk and Safety. *Acta Psychologica*, 56(1-3), 183-203.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & security, 24(2), 124-133.

Tsuchiya, S. (1993) Improving knowledge creation ability through organizational learning, in ISMICK 1993: Proceedings of the International Symposium on the Management of Industrial and Corporate Knowledge, 87–95.

Turner, D. W. (2010) Qualitative Interview Design: A Practical Guide for Novice Investigators. *The Qualitative Report*, 15(3), 754-760.

Viljanen, L. (2005) Towards an Ontology of Trust. In: Katsikas, S., López, J., & Pernul, G. (eds) *Trust, Privacy, and Security in Digital Business. TrustBus 2005. Lecture Notes in Computer Science, vol 3592*. Berlin/ Heidelberg, CH: Springer, pp. 175-184.

Weinstein, N. D. (1980) Unrealistic Optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806-820.

Whitman M.E., Mattord H.J (2011) Principles of information security, 4th Edition, Cengage Learning.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 1-20.