Organization Members Developing Information Security Policies: a Case Study

Hanna Paananen
University of Jyvaskyla, hanna.k.paananen@jyu.fi

Mikko Siponen
University of Jyväskylä, mikko.t.siponen@jyu.fi

Organization Members Developing Information Security Policies: A Case Study

Completed Research Paper

Hanna Paananen
University of Jyvaskyla
PO Box 35
40014 University of Jyvaskyla
Finland
hanna.k.paananen@jyu.fi

Mikko Siponen
University of Jyvaskyla
PO Box 35
40014 University of Jyvaskyla
Finland
mikko.siponen@jyu.fi

Abstract

Information security policies (ISPs) have a key role in organizational information security. Research has introduced processes for ISP development, including lifecycle models. There are also recommendations to include contextual issues in the ISP development to ensure that the ISP provides tailored protection to the organization's assets. One way of ensuring this is to include organization members in the development efforts. We identified six functions for the organization member participation from the research literature. Then, we presented two case studies of organizations where the personnel was included in the ISP development process. We found that the participation of the organization members did add value to the process through these functions but that there were also some negative effects. The inclusion of organization members in ISP development can help in gathering feedback directly at the beginning of the lifecycle without the need to go through the entire cycle to identify issues.

Keywords: Information security policy development, case study

Introduction

Organizations use information security policies (ISPs) to prepare and defend against the devastating effects of such information security incidents or attacks (Cram et al., 2017). ISPs direct employees to use information assets in a way that protects them and allows the organization to operate as desired (von Solms et al., 2011). The failure to do so has motivated ISP research to focus on studying awareness and compliance issues (Cram, et al. 2017; Moody et al., 2018). However, it has been found that non-compliance may stem from cumbersome policies, which lead to workarounds and declining motivation toward information security (Karlsson et al., 2017). Policies may even be in conflict with work objectives or impossible to follow (Balozian et al. 2023; Niemimaa & Niemimaa, 2019).

Aligning the ISP with work practices requires considering many contextual factors (Karyda et al., 2005). Many ISP development methods propose that organization members could be included in creating an ISP to achieve this (Flowerday & Tuyikeze, 2016; Karyda et al., 2005; Knapp et al., 2009). Previous research has found that user participation benefits system risk management (Spears & Barki, 2010). However, how to best include organization members in the ISP development process is not largely discussed in the ISP development literature (Rostami, 2019). Few research publications have discussed the practices of including organization members and their effects on ISP development and implementation (e.g., Niemimaa, 2016). Some researchers have proposed including employees as a way of solving value conflicts

when they arise from differing goals of work and information security (Burgemeestre et al., 2013; Hedström et al., 2011).

There are general recommendations for organization member involvement, but we know little about how they are turned into actual practices of participation. The goal of this research is to examine what functions organization members may have in the ISP development process and how these functions emerge in the practices of the work. The answers to these questions are sought through two case studies.

This article is structured as follows. First, the research literature on ISP development, context, and organization member involvement is discussed. Then, two cases of ISP development processes are presented and analyzed. Lastly, the implications of the research findings are discussed.

Previous Research on ISP Development

Over the years, ISP development has been studied in the realm of information security management (Cram et al., 2017; Paananen et al., 2020). ISPs are often divided into two interconnected categories: technical and managerial (Baskerville & Siponen, 2002). ISPs often refer to a collection of documents on different levels of abstraction, from top-level strategic (or even philosophical) statements to task-specific detailed guidance and implementation rules (Cram et al., 2017; von Solms et al., 2011). In general, the ISP steers or changes how an organization handles information, indicates the subjects and objects of the rules and prepares the organization to prevent and endure information security incidents (Baskerville & Siponen, 2002; Paananen et al., 2020). The ISP development process needs to address these different aspects of the policy. The following sections will first introduce some general lifecycle models recommended for ISP development. We then move on to discuss their relationship with specific contexts. Finally, we will discuss the effects of organization member participation on the ISP development process.

ISP Development Processes

In terms of method or process, ISP development is often described as a lifecycle model in which the previous cycle feeds into the next cycle of development. Paananen et al. (2020) compared several ISP development models and found that the content creation phase is usually preceded by an assessment (e.g., risks) and followed by phases relating to implementation and maintenance. These phases are also the foundation of the Policy Framework for Interpreting Risk in E-Business Security (PFRIES) model, which is presented with practical advice on how ISPs should be developed (Rees et al., 2003). Another example is an ISP lifecycle model presented by Flowerday and Tuyikeze (2016), which has five steps: risk assessment, policy construction, policy implementation, policy compliance, and policy monitoring. The lifecycle model by Knapp et al. (2009) was developed using an open-ended questionnaire for security professionals. This model differs from the previous example by having approval and training before policy implementation and enforcement and includes a review at the end of the cycle.

Figure 1 depicts a generalization of these lifecycle models. The requirements and assessment include assessing existing policy, listing external and internal requirements, and assessing risks (Knapp, et al 2009; Rees et al. 2003). The development phase includes the actual creation of the content of the ISP, during which there may be several iterations back to the assessment phase (Knapp et al. 2009). The development is followed by testing and approval (Baskerville & Siponen, 2002; Knapp et al. 2009), and the most important function of this phase is to freeze the content of the policy for the following implementation phase. The implementation phase includes making technological and managerial changes according to the policy (Paananen et al., 2020). Lastly, the ISP is in full operation, and its effectiveness can be monitored (Knapp, et al 2009; Rees et al. 2003). Ideally, this phase should continue for some time without emerging needs to revise the policy, and the new cycle could be started from a planned review. The ISP content is in a state of change in the phases depicted on the right side of Figure 1 and unchanged on the left-hand side.

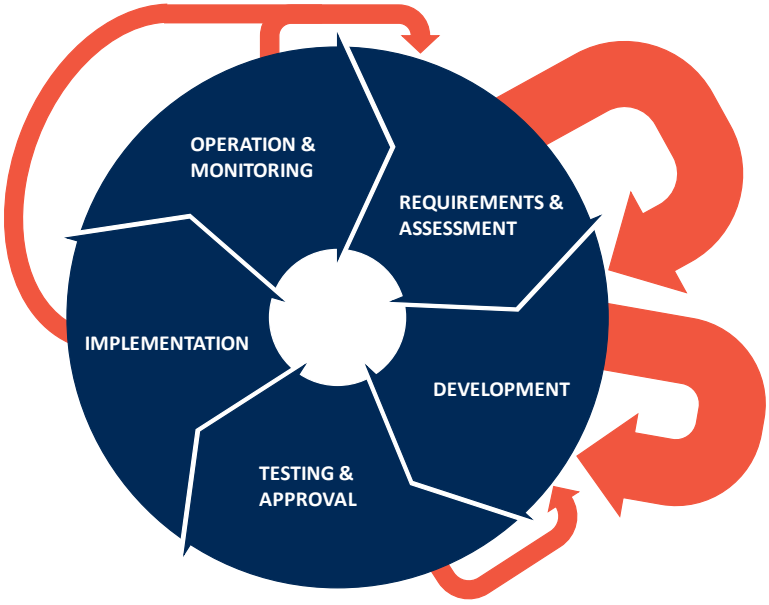

Figure 1. ISP lifecycle with feedback loops

These lifecycle models also mention internal and external influencers in the process. Internal influencers include management and employee support, organizational culture, business objectives, the technical environment, and identified threats (Flowerday & Tuyikeze, 2016; Knapp et al., 2009). In addition to these, Karyda et al. (2005) identified other contextual factors, including organizational structure, security officer, training and education, contribution to users' goals, and users' participation in the formulation process. Research has shown that the lack of organization member involvement in the assessment and development phase can lead to failure in implementation where the employees do not know or follow the policy (Lapke & Dhillon, 2008). The high-level processes and influencers of ISP development can provide an overview of the role of organization members but lack the details of how these concepts emerge in specific contexts. They do not address what stakeholders actually do in the process or how it affects the process.

The Context of ISP Development

Since every organization has specific or many unique characteristics regarding its business goals, people, processes and/or technology, it is often recommended that ISPs are expressly developed to protect the information environment where they are linked. Organizations may use the same technologies, which warrants the adoption of similar controls, but the combination of selected controls should always match the context. (Doherty & Fulford, 2006; Karyda et al., 2005; Siponen & Willison, 2009) The ISP literature sometimes calls such context-aware ISP development organization-specific policy development (Baskerville & Siponen, 2002).

Contextual factors are often recommended to be included in the ISP development in the phase of requirements gathering and assessment of the current situation (see Figure 1). External threats, industry regulations, security standards, and best-practice documents all influence information security policy in an organization (Flowerday & Tuyikeze, 2016). These external issues can motivate the selection of a more preventative or responsive ISP design (Baskerville et al., 2014). However, the greatest influencer in top management's steering of information security issues seems to be mimicking peers (Hassandoust et al., 2022). The orange feedback loops in Figure 1 signify how learning about contextual factors in different parts of the ISP development cycle can feed new information to the assessment and design of the ISP. In the PFRIES model (Rees et al., 2003), feedback loops are drawn from each step to the previous one, and their function is to make sure that the requirements of the phases are satisfied. In Figure 1, they are drawn away from the approval phase that "freezes" the content towards the assessment and development phases where the content changes. The arrows here resemble the Knapp et al. (2009) model, where the arrows are drawn as two-ended between the phases where the change happens.

A comprehensive view of contextual issues in ISPs can also affect employee ISP compliance in the operation phase. Aurigemma and Mattson (2019) critiqued the common approach in the ISP compliance literature that does not acknowledge the differences in ISP content areas but instead draws generalizations of compliance from one threat or countermeasure-specific rules to all ISP compliance. Their research showed that there are differences in behavior (or intention) dependent on the type of threat-specific ISP rule. Their findings give reason to expect that the employee/user point of view could be important in several areas of ISP development instead of generalizing their requests or ideas from one area to another.

Including Organization Members in ISP Development

One aspect of the ISP development process is the people who participate in creating or evaluating the content of the policy. The information security officer usually plays the main role (Karyda et al., 2005; Maynard et al., 2011) and seems to be the target of most advice. Many authors mention executive support and user participation (Maynard et al., 2011; Rostami, 2019), and some recommend organizational roles that should be included in the development team, such as "human resources, legal and regulatory matters, information systems, public relations, security, and the various lines of business" (Rees et al., 2003, p. 102). Participation from different units is expected to ensure that the policy is adaptable to all business areas (Flowerday & Tuyikeze, 2016). This also helps in understanding the ISP's target subjects (Baskerville & Siponen, 2002).

The ISP development lifecycle starts with assessing the current situation and understanding external requirements from the organization's point of view, followed by the design and development of the policy (Karyda et al., 2005; Paananen et al., 2020). At the beginning of ISP development, there is a need to identify the security objects or information assets of the organization (Baskerville & Siponen, 2002). Employee participation is recommended in this phase since the computers they work on and the information they process in their daily work are significant assets (Flowerday & Tuyikeze, 2016). Information flows in the processes are vital to business operations, and employees can help in understanding the information architecture, which is important in ensuring the security of these processes (Soomro et al., 2016).

In the ISP development phase, users have the possibility to reflect on how the different information security rules would affect their work (Albrechtsen, 2007). Users' expertise in the work processes and application domains can help in building security solutions (Siponen, 2005). Security controls should be planned in collaboration with end users to avoid too rigid controls that lead to workarounds (Colwill, 2009). Employees can also help identify conflicts between information security controls and business needs, and they may even come up with innovations that can solve conflicts between different demands (Burgemeestre et al., 2013; Hedström et al., 2011). When users contribute towards the management of information security risks in their work processes, they may pay more attention to ISPs and find the rules more appealing (Spears & Barki, 2010).

Organization members create and enact organizational culture, which again affects how policies are followed (van Niekerk & von Solms, 2010; da Veiga & Eloff, 2010). If the organization's culture is very individualistic and members are accustomed to making choices related to their work, the implementation of new security rules might fail if they are not involved in creating these rules (da Veiga & Eloff, 2010). Involvement helps in building buy-in, and this kind of "pull" to comply with the ISP has been shown to work better than "pushing" people with rewards and punishment (Flowerday & Tuyikeze, 2016; Sommestad et al., 2014). Information security rules have a major effect on people's daily work, and participating in their development can increase the sense of workplace democracy (Niemimaa & Niemimaa, 2019).

The reasoning behind including different members of the organization to design the ISP often relates to creating a common understanding and agreement on information security. When there are conflicts between different goals or values in ISP development, it may be difficult to find a mutual understanding that would best serve the organization (Burgemeestre et al., 2013; Hedström et al., 2011). However, uncovering these conflicts might be difficult if people do not share the same conceptualizations of the matter at hand. The organization members participating in ISP development need both personal capabilities and a shared understanding of concepts to reach a consensus on the requirements for the ISP. Good personal capabilities can lead to contextual factors, such as contributions to users' goals or education (Karyda et al., 2005). Shared social capabilities could lead to a change in organizational culture (Karyda et al., 2005; Knapp et al., 2009).

ISP documentation is primarily a communicative object (Karlsson et al., 2017). Collaboration in developing it helps to create a common language and tools for information security-related matters, which again contributes to an ISP that is easy to follow (Albrechtsen, 2007; Flowerday & Tuyikeze, 2016). Users can help in creating documentation that is easy for them to understand and covers all necessary areas but is not too long to read (Goel & Chengalur-Smith, 2010). A common language helps to form a shared understanding of information security issues and exposes the rationalizations behind decisions (Hedström et al., 2011).

ISP development is only one part of successful information security management, and fostering good collaboration practices between people is also beneficial to the later stages of the ISP lifecycle. The ISP development process can aid in creating a working relationship between representatives of different business areas and information security professionals (Albrechtsen, 2007). It is beneficial to communicate and absorb knowledge about information security benefits from prior experiences with the matter (Spears & Nicolas-Rocca, 2016).

Organization members in the ISP development lifecycle

Organization member participation can have benefits in different parts of the ISP life cycle. In a traditional view, the organization members are mostly involved with the ISP in the implementation and operation phases, while the assessment and development are the responsibility of the information security officer. Monitoring the ISP effectiveness allows collecting requirements for the next assessment phase (Höne & Eloff, 2002; Von Solms, 2001). However, in the previous section, we have identified many functions for organization members that could benefit the assessment and development phases as well. The thick arrows in Figure 1 depict the idea of utilizing organization members' feedback directly in the phases when the ISP is in a state of change without going through the full lifecycle.

In summary, previous research has identified the following functions for organization member participation in the ISP development process :

- Identify ISP subjects (roles and stakeholders).
- Identify ISP objects (information assets).
- Identify conflicts between information security and business requirements.
- Contribute to personal learning and buy-in.
- Match the ISP to the organizational culture and create an information security culture.
- Create a common language and collaboration practices.

Organization member participation has been recommended in the research literature over the years. There are some studies that have focused on how participation happens in the practices of ISP development tasks (e.g., Burgemeestre et al., 2013; Hedström et al., 2011; Niemimaa & Niemimaa, 2019). They give insight into how higher-level process diagrams, such as the ISP development lifecycle, take place in day-to-day activities, such as fitting together local requirements and best practice recommendations (Niemimaa & Niemimaa, 2019). This type of practice-oriented research improves our understanding of the fit between the higher-level concepts and their usefulness in practice. In this section, we have identified a list of high-level functions that can be used to understand the effects of organization member participation in the ISP development process.

Case Studies

This research investigates organization member participation in ISP development at two medium-sized companies (150-250 employees) in a northern European country. The researcher worked with an information security consulting firm commissioned to run ISP development service processes at these two customer companies. The first customer (ManuCorp) operates in industrial component manufacturing, and the second customer (InfraCorp) operates in community infrastructure. Both companies were long-time customers of the consulting firm in other services. Medium-sized companies are an interesting research topic for information security management since they are large enough to require formal governance structures but too small to have a full internal information security unit. SMEs (Small and medium-sized enterprises) are a huge part of the economy, and in Europe, medium-sized firms alone employ 16% of the population and account for 17.1% of the value added (Eurostat, 2022).

Method and Data Collection

This study follows the principles of interpretive field study (Klein & Myers, 1999) and, particularly, case research (Benbasat et al., 1987; Pan & Tan, 2011). This paper covers projects in two case organizations that develop their ISPs with the help of the same consultant. This research approach was selected to acquire detailed data on organization member participation in ISP development, with a special focus on understanding how the concepts from the ISP literature are reflected in practice.

The research project was planned in collaboration with a consultant firm that offered an ISP development service to its customers. Organization member participation was discussed between the researchers and the consulting firm on several occasions before the projects started with ManuCorp and InfraCorp. The incorporation of a larger representation of organization members in the ISP development project was a new addition to the service that was intended to improve contextual requirements gathering. Although the researchers had discussions with the consultant, they did not control or manipulate the actual ISP development process (Benbasat et al., 1987). As the consultancy operated as a gatekeeper to the organizations, further data gathering beyond the joint meetings was not possible.

The research data consists of the seven sources listed below (Table 1). Due to the medium size of the organizations, the meetings listed here represent a major part of the ISP development lifecycle for these companies. In each workshop, there were 4–12 participants in addition to the consultant; thus, the data represent the views of over 30 people (Pan & Tan, 2011). The exact amount of participants was not always clear as several locations were connected via teleconferencing, and people did not always notify others when they joined in. Due to the size of the organization, the hierarchy was low, and in many instances, a person represented both top and middle management.

The consultant arranged the workshops and asked permission for the researcher to observe them. In the assessment workshops, the researcher participated by remote connection, and in the ManuCorp development workshop, they attended in person. All workshops and interviews were audio recorded and later transcribed and coded to identify themes recognized in the ISP development literature (Pan & Tan, 2011).

Company	Meeting content	Participants
ManuCorp	Assessment: modeling and assessing processes, 7 h	Heads of units, 10-12 participants
	Development: Selecting ISP content, 7 h	Heads of units, 10-12 participants
	Interview: evaluation of workshops, 1 h	Information security manager
InfraCorp	Assessment: ISP development process requirements gathering, 2 h	Heads of units, 8-10 participants
	Assessment: processes for the unit for product delivery, 2 h	Head of unit + 4 key personnel
	Assessment: processes for communications and PR unit, 2h	Head of unit + 3 key personnel
	Assessment: processes for sales and customer service unit, 2 h	Head of unit + 4 key personnel

Table 1. Description of the research data

Results

This section discusses the two ISP development projects, first the ManuCorp case and then the InfraCorp case. The data are presented in chronological order, although the InfraCorp representative interview took place after the ManuCorp project had started. Generalized terminology is used to protect the privacy and security of the people and organizations involved.

The ISP development service followed the same general structure across both customer organizations. First, the process assessment workshops were held for setting goals and describing work processes. The organization members were asked to describe their work at a higher process level and evaluate the criticality and the current situation of the process, especially from the information security point of view. After assessing the processes and any risks related to them, the service process moved to policy development workshops, where the consultant helped the customers select rules for their own ISP. The policy

development was largely based on the structure of the ISO 27002 standard but with a lighter approach since neither of the customers was looking to be certified in the near future. This approach meant that less effort was put into focusing on advanced or complex topics such as encrypting. With these areas, the consultant offered general baseline controls that suited SMEs. However, all main areas of the standard were presented to the customers to give them the opportunity to include or omit sections as they saw fit.

ManuCorp

At ManuCorp, the first assessment workshop covered evaluating all processes in the company. The participants were heads of units and two consultants: an IT (information technology) service consultant and an ISP development consultant who facilitated the workshop. The ISP consultant had asked the ManuCorp information security manager to invite representatives of all business areas to the workshops, and over 10 participants attended, in addition to the two consultants. The participants came from all teams and business locations of the firm and thus had first-hand knowledge of all major processes.

ManuCorp had previously mapped some processes with the IT consultant in relation to other IT-related services. This led to the first part of the workshop being a dialogue between the IT and ISP consultants, while the customer representatives mostly just agreed on what they were proposing. The ISP consultant asked whether it would be better to map the processes from ManuCorp's point of view instead of the service provider's, but the customer representatives did not see the importance of that.

When the conversation moved away from IT, the ManuCorp employees started to take part more, even though it still required many very precise questions about working practices. For example, purchase orders were first described as a process conducted within specialized software and not very critical for information security. Further questions revealed that the orders were sent out by email, leaving room for human error. The documents attached to the emails could include quite sensitive business information such as product specifications and prices. This was one of the instances where the consultant thought the business criticality of the process was higher than what the participants evaluated.

After spending a few hours going through the first process groups, the participants started to come up with their own ideas. For example, missing processes were identified that were not part of the other high-level processes in the process group. As the participants grew more familiar with the working method, the process evaluation became faster. The quick pace also seemed to lead to less focus on details. The participant who was responsible for each process group might make quick estimates of the processes' criticality without much explanation. At some points, the consultant would ask them to further explain why they thought a process was critical from an information security point of view, and the participants were not able to explain what kind of information made the process critical. By contrast, processes, where personal information was used, were given higher criticality estimations since the participants knew that information needed special protection by law. Overall, it seemed that identifying ISP subjects and aspects of the business requirements was easier than identifying ISP objects.

After the assessment phase, the ISP development project moved on to the development phase. The ManuCorp policy development workshop had over 10 participants in three company locations (people in three meeting rooms connected to an online meeting). They represented different units, including the top management of the company. The workshop lasted for the entire workday and covered several areas of the ISO 27002 standard. The workshop started with the consultant asking the participants why they chose to start developing a comprehensive ISP. The ManuCorp information security officer answered that they did not have any overarching control over information security in the company, and, for example, the legislation concerning private information (EU GDPR, general data protection regulation) needed to be considered. Other participants commented that there was a need for a "wake-up call" to make the organization more information security aware.

The consensus on choosing controls was that they should not complicate daily work routines in any way, and taking risks was better than sacrificing convenience. The tone of the conversation changed to stricter control when discussing the rights to ManuCorp-generated business information or immaterial property rights (IPR). Due to a previously experienced dispute over IPR, ManuCorp wanted very tight controls over this information that could only be subverted with tight contracts. Another good example of a remark made by the managers regarding ISP development often becoming relevant when there are incidents was, "If a customer calls to say, 'by the way, you have a 10-million-euro claim coming your way'". This shows that the

management was motivated not only by a reputation risk but also by the financial consequences of security breaches.

The participants considered customer information to be the most important thing to protect with an ISP. Although ManuCorp was a medium-sized firm, its customers included global businesses that had demands that needed to be taken into consideration in all business processes. ManuCorp was also a consolidated company with different units that had very different ways of working. Some employees stayed in place at the manufacturing facilities, while others did very mobile work, and these differences needed to be incorporated into the ISP.

"A few years ago, the CEO lost their laptop somewhere."
"Lucky it was the CEO, so there was probably nothing sensitive on it."

Understanding the scope of ISP development was equally difficult for the participants and the consultant. When the consultant asked about managing partner relations, the purchasing manager proclaimed that he knew nothing about the IT partners—only the suppliers of production. When it was clarified that the ISP would need to cover all information exchange with all business partners, the manager said that they had no common instructions on what information they could share; instead, he would use common sense in determining how much detail could be shared with external parties.

The topic of segregation of duties was mostly dismissed with an appeal to the small size and low organizational structure of ManuCorp. One manager said, "We are not aiming for the American control over the trust system but for the trust over control." Similarly, when mobile devices were discussed, it became clear that employees working on customer sites used shared devices that were not password protected. A manager stated that it was a risk they took when they decided to test the use of these devices. In both instances, the participants knew that these situations usually had tighter information security controls, but they chose convenience. The consultant wrote down all these decisions and moved on to write the ISP after the development workshop.

The ManuCorp information security manager was interviewed after the development workshops but before the final approval of the ISP. It was his responsibility to run the project with the consultant and ensure that the organization members participating in the workshops were representatives of the different business areas of the organization. He thought that having large workshops of over 10 participants was too big, and 20–30% of the participants did not feel that the discussion was related to their work and were frustrated. People also lacked an information security mindset, which led them to focus on unrelated issues. However, as the consultant steered the conversation with a set of questions in different content areas, it helped to focus on the task at hand. There were also some differences of opinion when the consultant suggested a laborious information classification scheme, but the organization members thought that they needed a lighter approach for it to be implementable. Most content areas did not cause much conversation or conflict, and the information security manager thought that for many participants, this was not a learning experience, even if some might have had some new realizations. There was a need for education, however, since the personnel did not have the capability to adequately protect their customer information.

InfraCorp

The ISP development project started at InfraCorp with a meeting with the consultant and leaders of different business units. The meeting started with a long explanation from the CEO about why he thought entering into this process would be beneficial to the company. He explained that as a provider of the communal infrastructure, he thought it was their duty to be prepared against cyberattacks to avoid causing harm to society. His hope was that the process would teach them about good practices and support the competencies of their own IT staff. He and the consultant also had a dialogue about calculated risk-taking as a part of understanding the alignment of business and information security.

After the CEO had motivated the reason for the project, the consultant explained how the process would move forward to process assessment workshops, followed by ISP development workshops. The participants were worried that the right people would not be invited to the assessment workshops and that they would need to do new process maps, even though they had just drawn some. The consultant explained that they could invite anyone to the assessment workshops since they would be held separately for business areas.

One participant also inquired about including processes that span organizational boundaries, to which the consultant answered that partner relationships would only be addressed in the ISP development workshop.

The three process assessment workshops at InfraCorp had fewer participants than the ManuCorp workshops. Here, the process workshops were arranged separately for each unit, and a large portion of the personnel of these units participated in their workshop. Like ManuCorp, InfraCorp also had previously mapped processes in the consultant's systems, but the process map was not complete. The first business unit workshop started very efficiently, with a participant listing the main processes of the unit right offhand. As the process mapping continued, the descriptions quickly became very detailed, and the consultant asked the participants to focus on the level needed for information security. This led the participants to consider the personal information that was transferred in these processes and to think of the different levels of threats. In this instance, the consultant asked them to focus more generally on the information that was processed and not only personal information.

After naming the main processes of the unit, the consultant asked about the business criticality of the processes. Some of the participants had trouble grasping what the scale of critical–important–supportive meant. The consultant came up with timeframes for how long the process could be down without significantly affecting the business. The most challenging task for the participants seemed to be evaluating the confidentiality, integrity, and availability (CIA) situation and the need for each process. These terms needed clarification from the consultant.

The second process workshop started with questions about defining processes that exist independently but are also part of many other processes. The participants had difficulties separating support processes from the core processes they served.

"Do you have a process for planning and carrying out customer communication?"
"Well, you could call me a process…"

In the second workshop, the consultant had to continue defining terms for the participants, but this time, he was ready for the questions. Regardless, the word "integrity" in the sense of processing information was very hard for the participants to grasp. They became frustrated with the difficulties in defining and evaluating the processes. They wrote the definitions of confidentiality, integrity, and availability on a flip chart to be able to return to them on every item. The consultant tried to explain that these refer to the information that the process uses. Once the participants had spent a while learning the concepts, they quickly gave these evaluations to all other processes.

"Can we just stop doing it if we don't know how?"

The third workshop began with a review of the processes mapped in the previous workshops. This unit wanted to list the same processes from its own point of view, which happened very quickly compared to the first workshop. The pace slowed when it was time to evaluate the CIA values for the processes. The group was ready to evaluate one process of having good availability until it became clear that the systems used in the process were often down for short periods of time. Matching their processes to the other units also brought difficulties in defining them. One participant noted that if each unit should describe their processes only from their point of view, then there was a danger of leaving gray areas between the units' responsibilities. The consultant explained that their expectation was that the named process owners would handle any issues they detected.

Summary of the Results

The results of this case study highlight the same functions for organization member participation that we previously identified in the research literature (p. 5). Next, we provide a summary of the results from both case organizations using the themes from the literature. This section is concluded by Table 2, which further summarizes the key findings.

Identifying ISP subjects was a major part of the process through engaging organization members and naming people responsible for the processes. However, the focus was on people as informants rather than on people as actors in information security. Selecting informants was also not easy. The ManuCorp representative was given the task of inviting people to the workshops with little familiarity with the process

or with what benefits were expected from organization member participation. InfraCorp had assessment workshops for each business area, allowing more participants and better visibility of what different employees do in each unit. A participant identified subjects outside organizational boundaries, but they were not addressed in the assessment workshops and were only lightly touched as a contractual issue in the development workshop.

Identifying ISP objects was done mainly through discussing processes. Due to outsourcing IT services, ManuCorp had a limited understanding of the importance of its IT assets to its processes and information security. It was difficult for the organization members to identify information in the processes beyond personal data. Creating a comprehensive overview of the organization's processes was demanding, and having several units working on them created the risk of leaving gray areas. The evaluation of the processes also proved laborious, as understanding the significance of the CIA values was hard for the participants.

Identifying conflicts between information security and business requirements was the main motivation for conducting comprehensive process mapping. This was impeded by the participants' limited views of information security. At ManuCorp, a clear statement was made that business requirements take precedence. Taking calculated risks was also preferred at InfraCorp over limiting ISPs. ManuCorp had demands from their customers about good information security posture but no skills to turn the requirements into policies and further into practices. IPR was especially important for ManuCorp, which led to the selection of particularly tight rules on the matter.

Contributing to personal learning and buy-in are important from the ISP lifecycle point of view since they are considered to create a better posture for the later implementation and maintenance phases. At the ManuCorp assessment workshop, creating buy-in for the ISP development process was not very successful. The lack of connection between the workshop content and one's own expertise caused a low level of learning and few new insights. In the InfraCorp assessment workshops, we could identify instances where participants started to understand the information security aspects of their work and plan for improvements. Consultant-led ISP development processes also provided master–apprentice type of learning to the organization's own information security officers.

Matching the ISP to the organizational culture and creating an information security culture became a large part of the process when people were repeatedly asked how they wanted things done in their workplace. The consultant made it clear that he could not decide what was best for the organization, and instead, the organization members needed to take responsibility for the information security decisions. The development process worked as a wake-up call to pay more attention to information security. The CEO at InfraCorp motivated the ISP process by appealing to the organization's duty to protect society from disturbances in infrastructure.

Creating a common language and collaboration practices were the biggest barriers to progress. CIA evaluation requires the ability to conceptualize information in a particular way that is not necessarily shared across organizations or professions. While creating common understanding took time in the assessment workshops, they also taught the organization members to describe their information use through processes.

Function	Key findings
Identifying ISP subjects	• The information security manager could not identify all key personnel and mostly focused on formal structures (managers) • The participating organization members could identify key actors.
Identifying ISP objects	• Major difficulties in identifying information that processes use • Understanding the significance of CIA values in completing processes was difficult • Process discussions allowed forming a view of the information beyond IT systems
Identifying conflicts between information security and business	• Concerns about information security restricting business were raised • The business importance of information was shared through cautionary tales

Contributing to personal learning and buy-in	• Buy-in to the process was created when the topic of discussion was related to one's own work. • Master-apprentice learning between consultant and information security manager
Matching the ISP to the organizational culture and creating an information security culture	• The reliance on outside authority shifted towards taking collective responsibility. • The significance of information security could be connected to the mission of the organization.
Creating a common language and collaboration	• Introducing new terms (to both the organization members and consultant) required time. • Describing processes made it clearer how the key personnel needed to consider information security processes.

Table 2. Key findings

Discussion

Organization members are often mentioned as a valuable resource in the ISP development literature, but the practices of their inclusion in the process are rarely discussed. The two case studies in this article provide a detailed description of how organization members can be involved in ISP development in practice. The results shed light on not only the benefits of organization member participation but also the drawbacks.

In this study, we concentrate on employee participation in the assessment and development phases of ISP development (as part of an ISP lifecycle depicted in Figure 1). The employees have different functions or tasks in these phases with the aim of improving the resulting policy. The lack of employee input in ISP development has been previously connected with problems in implementation and the capacity of the ISP to shield the organization from information security incidences (Lapke & Dhillon, 2006). In terms of timeline, discovering weaknesses in the ISP during the operation phase means that the entire life cycle, and probably several months, have passed before the requirements for the ISP were discovered. While the idea of a lifecycle is continuous improvement, the security posture of the organization may stay dangerously low if feedback on the applicability to the context is not efficiently utilized at the beginning of the cycle. This view is in line with previous ISP development literature (e.g., Knapp et al. 2009). This research examined the use of organization members to increase the amount of feedback in the first phases of the life cycle (see thick orange arrows in Figure 1).

The employees or managers of the organization are often described as influencing factors in the ISP development process (e.g., Flowerday & Tuyikeze, 2016) rather than actors with clear tasks. To obtain the benefits of organization member participation, deeper understanding has been called for regarding how and in what phases they should be included (Maynard et al., 2011). In this study, we can identify similar tasks for different roles, as have been previously presented in the literature. For example, the executive manager had the task of motivating organization members to change their work practices to more secure ones (Karyda et al., 2005). However, the same managers were the loudest advocates for the business-first type of thinking, which would have added ambiguity to employees' minds about the kinds of behavior that please management. Managers' role in aligning information security strategies (McFadzean et al., 2007) and using power (Lapke & Dhillon, 2008) has been studied, but this finding also puts forth the need to guide the top management participation toward the functions that would not have such detrimental effects. For example, promoting the personal learning of managers during the process could positively affect their future information security decisions. This could help in mitigating the lack of understanding that can be a barrier to including information security in the high-level decision-making of the company (McFadzean et al. 2007).

The assessment workshops were held to gather knowledge about the operations of the organizations. This approach produced valuable information about the processes and responsibilities and helped the workshop participants see their work from the information security point of view, which is one of the expected benefits of organization member participation. However, these workshops assessed only a small portion of the internal and external influencers of ISP development identified in the literature (Knapp et al., 2009). Further, this approach was not a perfect fit with the next step of the ISP development process, which used

the ISO 27002 standard. The assumptions of governance styles and information assets were different in these two phases, which diminished the benefits that could be gained from either step. This is in line with previous research that found that standards provide weak support in adapting their recommendations to local contexts (Niemimaa & Niemimaa, 2019; Siponen & Willison, 2009).

Identifying value conflicts between business and information security requirements is one of the main reasons why organization member participation in ISP development is found to be useful (Burgemeestre et al., 2013; Hedström et al., 2011). However, this requires a thorough understanding of both worlds. Gathering and analyzing this information is a mammoth job that organization member participation can aid by ensuring that all aspects are covered, and organizational needs are met. However, based on this research, it seems that the extent and importance of the workload are understated in ISP development recommendations. What is especially lacking are indicators for quality that could be used to understand when the assessment is comprehensive enough to move on to the development phase. This is not to say that we would advocate rigid process models but that in any development style, developers should try to reach a common understanding of the situation. With the contextual view of ISP development, this can be achieved only by a deep understanding of the setting and not solely through external recommendations or checklists, which can cause gray areas (Siponen, 2005; Siponen & Willison, 2009).

The policy workshop at ManuCorp was a good example of how the ISP could be adapted to an organizational culture. The managers who had worked in the company for a long time mentioned that quite often, they tended toward "business first" and knowingly took risks. To avoid too rigid controls after the ISP was in place, they chose to leave out many of the recommended controls in ISO 27002. Instead, they chose goals that would be easy for them to achieve. These decisions seem to reflect an organizational culture in which the most important thing is to get things done. A different kind of organization might have chosen almost unrealistic goals and focused more on the journey toward achieving them. The perception of risk and the importance of IT have been identified to influence information security strategy development in executive boards (McFadzean et al., 2007). Here, we can detect the strategizing taking place throughout the ISP development process.

The ineffectiveness of complicated ISP documentation has been noted in prior research (Goel & Chengalur-Smith, 2010; Karlsson et al., 2017). The InfraCorp workshops illustrate how common language is developed during the ISP development process. In the first workshop, the definition of a good abstraction level for the processes was difficult for the participants. The consultant also had trouble explaining how to perform the evaluations for each process. In subsequent workshops, the participants mimicked the processes that had already been defined. The consultant was also better prepared to explain how the evaluation was supposed to be done using examples. This shows that concepts such as a process or CIA values may be easy to grasp for someone who has had training in information systems but may be hard to grasp for people with different backgrounds. The function of the organization members here was to give feedback on the incomprehensible wording to the consultant during the development process. Sharing an understanding of even the simplest concepts through collaboration and examples could help create a common language that effectively communicates the intentions of the ISP documentation. A similar phenomenon was uncovered by Niemimaa and Niemimaa (2019), who found that abductive innovations were needed to match the wording of a standard to a local context. As the forming of the middle ground between the local context and the general best practices may need negotiation, it might be advisable to reserve time for learning key concepts from the beginning of the project.

There were several instances in the workshops in which the participants treated the consultant as if he were the holder of "right" answers to questions. The first instance was during the very first workshop, which started with the consultants talking to each other and the organization members passively listening. A similar situation arose when workshop participants asked if they could describe their processes in a certain way. While respecting the expertise of a professional is wise, in this instance, it might have caused a false sense of security. Building a working relationship between the security officer and the rest of the staff requires close attention to the power relationships between them (Lapke & Dhillon, 2008). Further, too much reliance on the security officer may lead to a situation in which organization members do not take responsibility for dealing with information security issues since the information security officer is expected to do it all. This could be remedied with mutual learning where not only the organization members try to learn about information security concepts, but the information security officer tries to learn about the significance of information to the work of the organization members.

Overall, including members from different parts of the organization in the workshops seemed to create an interest in information security issues, and many participants suggested more secure ways of working even before the ISP was ready. In addition to personal interest and learning, the participants started to look at the organization and its social structures from an information security point of view. Within the ISP development lifecycle, this has benefits in forming awareness for the maintenance phase, but it also builds competencies toward the next ISP revision cycle. Generating and leveraging this ISP development competence within the organization does, however, require skillful planning from the leader of the ISP development effort. The six functions of organization member participation presented in this paper can be used to plan the inclusion of employees in the ISP development process. The results also highlight difficulties that may not be avoided, but they may be considered in advance.

Limitations

The two case studies presented in this paper represent only the assessment and development phases of the ISP lifecycle. Although gaining an understanding of the practices in these phases is important, it does not allow us to make any assumptions about any of the other phases. It has been suggested that organization member participation could build buy-in that would help in the implementation and maintenance phases, but this research provides no evidence for that. We are not able to conclusively say that organization member participation improved the ISP development process since there is no data about a process in which they did not participate.

Another limitation (or strength) of this paper is that it investigates medium-sized enterprises. Some of the interpretations we make of the data may be connected to the size of the organization. The people involved in the ISP development process personally knew every member of the organization. In a larger organization, the effects of security culture and creating a common language may be quite different if the percentage or intensity of participation is different from this study.

Future Directions

Future research should continue to focus on ISP development practices and the people who enact them. In this paper, we tried to illustrate the complex interactions that take place in the assessment and development phases of the ISP development lifecycle. There are many of these conceptual models in which high-level tasks follow each other, usually in very similar ways. Gaining a further understanding of how these abstractions turn into daily tasks and interactions could reveal new insights into successful ISP development. For example, simplified views of defining information assets can lead to inadequate risk assessment and selecting controls that do not sufficiently protect information. The reasons for this may lie in people's learning, cognition, ethics, or social behavior. Longitudinal studies connecting different phases of the ISP development lifecycle could shed light on the chains of actions that happen before the success or failure of information security efforts.

The idea of connecting certain ISP development practices with the effects that an ISP has on information security is complex and has not been comprehensively addressed in empirical research. As many authors promote the idea of contextual ISPs, it may not even be desirable to create an overall theory of ISP development that could cover all mechanisms related to context. More important would be to question the underlying assumptions of current approaches and produce field research that better explains how different practices contribute to the success of ISP development. This research touches on the discussion of the firm size and applicability of best practices (in this instance, ISO27002 standard), which still require more research. Further, the big question of how ISP development contributes to the lack of security breaches is unanswered and should be addressed, as difficult as it might be.

Conclusion

This article describes how organization members can be included in ISP development. Their participation is recommended in several phases of the ISP development life cycle, but the practices of how this is done are rarely discussed in the literature. This research focused on the assessment and development phases of the ISP lifecycle. The idea behind the lifecycle models is that they work iteratively, providing feedback from the previous cycle to the next. However, waiting for user feedback until the end of the cycle can take time

and put the organization at risk while issues are not identified. The inclusion of organization members in the early phases of the cycle allows for feedback to be included in the design before implementation.

Two case studies were presented to give a detailed account of what functions organization members can have in ISP development and how their functions can be identified in the practices. The cases were compared to the different functions of organization member participation found in previous research. Overall, the expected benefits of organization member participation were present in the case companies, although some practices also had potentially harmful effects that should be addressed when planning ISP development.

There are benefits to including organization members in ISP development, such as providing detailed knowledge about the context, forming shared language, and gaining an information security mindset. However, the demanding task and mixed messages from authorities may be unmotivating. Thus, including organization members requires specific skills from the project leader (often the information security officer or consultant). The leader must clarify the objectives of the inputs that are expected from participants and who might provide this insight. Secondly, the leader must know how to use different group work facilitating techniques to reach these objectives.

Acknowledgments

This research was funded by Business Finland and the Finnish Cultural Fund. We thank the reviewers of this paper for their valuable comments.

References

Albrechtsen, E. (2007). A qualitative study on users' view on information security. *Computers & Security*, *26*(2007), 276–289.

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, *20*(12), 7. **https://doi.org/10.17705/1jais.00583**

Balozian, P., Burns, A. J. & Leidner, D. E. (2023) An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures. *Journal of the Association for Information Systems, 24*(1), 161-221. **https://doi.org/10.17705/1jais.00798**

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337–346. **https://doi.org/10.1108/09576050210447019**

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. **https://doi.org/10.1016/j.im.2013.11.004**

Benbasat, I., Goldstein, D., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, *11*(3), 369.

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. H. (2013). Value-based argumentation for designing and auditing security measures. *Ethics and Information Technology*, *15*(3), 153–171. **https://doi.org/10.1007/s10676-013-9325-2**

Colwill, C. (2009). Human factors in information security: The insider threat – who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. **https://doi.org/10.1057/s41303-017-0059-9**

da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. **https://doi.org/10.1016/j.cose.2009.09.002**

Doherty, N. & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*(2006), 55-63. **https://doi.org/10.1016/j.cose.2005.09.009**

Eurostat. (27 June 2022). EU small and medium-sized enterprises: an overview. **https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220627-1**

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*(2016), 169–183. **https://doi.org/10.1016/j.cose.2016.06.002**

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, *19*(4), 281–295.

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information and Management*, *59*(1). **https://doi.org/10.1016/j.im.2021.103574**

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373–384. **https://doi.org/10.1016/j.jsis.2011.06.001**

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409. **https://doi.org/10.1016/S0167-4048(02)00504-7**

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers *and Security*, *67*. **https://doi.org/10.1016/j.cose.2016.12.012**

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security*, *24*(3), 246–260. **https://doi.org/10.1016/j.cose.2004.08.011**

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–94. https://doi.org/10.2307/249410

Knapp, K., Morris, F., Marshall, T., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493–508. **https://doi.org/10.1016/j.cose.2009.07.001**

Lapke, M., & Dhillon, G. (2006). A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study. *AMCIS 2006 Proceedings,* 166. **https://aisel.aisnet.org/amcis2006/166**

Lapke, M., & Dhillon, G. (2008). Power relationships in information systems security policy formulation and implementation. *ECIS 2008 Proceedings*. **https://aisel.aisnet.org/ecis2008/119**

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in security policy development. *Proceedings of the 9th Australian Information Security Management Conference*, 182–188. **https://doi.org/10.4225/75/57b546fecd8c6**

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, *31*(5), 622–660. **https://doi.org/10.1108/14684520710832333**

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), 285–311. **https://doi.org/10.25300/MISQ/2018/13853**

van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. **https://doi.org/10.1016/J.COSE.2009.10.005**

von Solms, B. (2001). Information Security – A Multidimensional Discipline. *Computers & Security 20*(2001), 504-508.

von Solms, R., Tomson, K. & Maninjwa, P. (2011). Information Security Governance Control Through Comprehensive Policy Architectures. *2011 Information Security for South Africa, Johannesburg, South Africa*, p. 1-6. **https://doi.org/10.1109/ISSA.2011.6027522**

Niemimaa, E. (2016). Crafting an information security policy: Insights from an ethnographic study. *ICIS 2016 Proceedings*. **https://aisel.aisnet.org/icis2016/Practice-OrientedResearch/Presentations/6**

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: An ethnographic study. *European Journal of Information Systems*, *28*(5), 566–589. **https://doi.org/10.1080/0960085X.2019.1624141**

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*(1), 1–14. **https://doi.org/10.1016/j.cose.2019.101608**

Pan, S. L., & Tan, B. (2011). Demystifying case research: A structured–pragmatic–situational (SPS) approach to conducting case studies. *Information and Organization*, *21*(3), 161–176. **https://doi.org/10.1016/J.INFOANDORG.2011.07.001**

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM*, *46*(7), 101–106. **https://doi.org/10.1145/792704.792706**

Rostami, E. (2019). Tailoring policies and involving users in constructing security policies: A mapping study. *Proceedings of the Thirteen International Symposium on Human Aspect of Information Security & Assurance*, Nicosia, July. **https://www.diva-portal.org/smash/record.jsf?dswid=3408&pid=diva2%3A1345646**

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*(3), 303–315.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. **https://doi.org/10.1016/j.im.2008.12.007**

Solms, R. von, Thomson, K.-L. L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security South Africa (ISSA), 2011*. **https://doi.org/10.1109/ISSA.2011.6027522**

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1).

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

Spears, J. L., & Nicolas-Rocca, T. S. (2016). Information security capacity building in community-based organizations: Examining the effects of knowledge transfer. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2016(March), 4011–4020. **https://doi.org/10.1109/HICSS.2016.498**