Security practitioners in context: Their activities and interactions with other stakeholders within organizations

ABSTRACT

Information security is a complex activity within organizations. This study develops the context of interactions of IT security practitioners, based on a grounded theory analysis of 21 interviews and participatory observation. We identify at least eight different activities that require interactions between security practitioners and different stakeholders. Lack of formal communications and ad-hoc reporting are recurrent sources of errors during these interactions. Our analysis also shows that tools used by our participants did not provide enough support for our participants to face the complexity of their tasks and the interactions required. Finally, we elaborate on different opportunities to improve the security tools used by practitioners. These tools need to provide better support to interactions and communications that security practitioners have with colleagues and other stakeholders.

ACM Classification Keywords

K.6.5 Management of Computing and Information Systems: Security and Protection; H.5.3 Information Interfaces and Presentation: Group and Organization Interfaces—*Collaborative Computing*

General Terms

Security Management, Design, Human Factor

Author Keywords

Tasks, Security Tools, Usable Security, Collaboration

INTRODUCTION

Information security has become a critical issue for organizations, which need to protect their information assets from unauthorized access and enable business activities after security breaches. Despite the amount of resources being spent on IT security, there is little empirical evidence on how human and organizational factors affect security effectiveness in organizations [1, 9, 15, 3]. In particular, literature on how IT security professionals interact and communicate in real contexts within their organizations is scarce [11, 2].

Botta et al [3] reported on the distributed nature of IT security responsibilities. They found IT security activities to be performed by groups that usually have a "coordinator", not necessarily a manager, who coordinates other IT specialists to perform IT security activities. Similarly, Kandogan and Haber [11] found that "security administration requires collaboration between people at many levels." Furthermore, Knapp et al. [13] identified the high level of interdependency of security tasks as "the extent to which individuals depend upon other individuals and resources to perform a job." However, none of these studies provide details on how security practitioners interact and communicate with other stakeholders within the organization, and how these interactions vary depending on the security activity being performed. As a result, Human Computer Interaction researchers and tool developers devoted to IT security lack an understanding of how to improve the tools and resources that IT security professionals need in order to interact effectively.

We take the perspective that human, organizational, and technological factors influence the ability of security practitioners to do their job well. So far, the field study has provided us two sources of data. The first source is 21 semi-structured in-situ interviews and questionnaires of security practitioners from both academic and private sectors. The second source is an ongoing participatory observation in one Canadian university. We are performing a field study to investigate methods and techniques for developing better tools for managing IT security

We analyzed the empirical data using grounded theory [5] focused on pre-designed themes. One of those themes was on how IT security professionals interact and communicate with other stakeholders. From our analysis of the participants' stories, details about the high dependency on communications and interactions to perform IT security tasks emerged.

The contribution of our study is twofold. First, we unpack the meaning of interdependency of IT security tasks, showing the different roles, communications and resources used by IT security professionals in real contexts. Second, with this better understanding of interdependency, we identified opportunities to improve tools that security professionals use to collaborate, cooperate, and coordinate with other stakeholders while performing their tasks. In the next section we discuss related work. We then present the design of our qualitative study followed by our results, discussion, and conclusions.

RELATED WORK

Empirical Research on information security (IS)

Kraemer and Carayon [16] identified and characterized elements related to human errors in the field of computer and information security (CIS). They used a macro ergonomic conceptual framework which was populated with qualitative data from 16 interviews of network administrators and security specialists. The analysis of the interviews showed that organizational factors, such as communication, security culture, policy and organizational structure were the most frequent behind information security errors. As Kraemer and Carayon, one of our objectives was to identify factors behind errors, although in our case these factors are specific for interactions of IT security professionals. Another difference, is that we were focused on how to evaluate and improve the tools and resources used by IT security professionals for interacting and performing their tasks. Our approach was also different; we are not using a predefined model to frame and map our findings.

Knapp et al. [13] investigated how to model those managerial constructs that most influenced the effectiveness of IT security. As part of their study, Knapp et al. surveyed 936 security professionals (CISSPs) with questions about the interdependency of IT security tasks . Knapp et al. concluded that security related tasks had a high level of interdependency. We departed from this result to understand in real contexts what interdependency means for security tasks, specifying how security practitioners had to coordinate and interacte with other stakeholders to perform their tasks. We also studied the tools that security practitioners needed during these interactions.

Computer Supported Collaborative Work (CSCW) on IS

Kandogan and Haber presented two different studies from ethnographic data related to IT security administrators [11], [9]. In the first one [11], they evaluated security administration tools: through 40 days of performing naturalistic observations of security administrators from a university in USA. Based on real situations faced by these security administrators, they gave recommendations about future developments of IT tools, including better visualization and correlation of anomalous events in the network. In the second study [9], they analyzed ethnographic data from 16 field studies of IT administrators in general to determine differences between IT administrators and IT security administrators. Kandogan and Harber' results inform our analysis and provide context to generalize and find particularities in our results. However, our goal is to provide not only recommendations on tools and particularities of IT security, but also a deeper understanding of the security practitioners' roles and interactions with other stakeholders within organizations.

Botta el al. [3] used grounded theory to identify the goals, responsibilities, tasks and tools used by security practitioners within organizations. The data in this initial analysis came from 14 interviews with security practitioners, with 12 of the participants from post-secondary educational and research institutions. We extend this work by providing details on how security practitioners interact within organizations.

Goodall et al. [8] reported on the expertise and collaboration necessary to administrate intrusion detection systems (IDSs). The data used for the analysis came from 9 semi-structured interviews of a diverse cross-section of intrusion detection experts. Goodall et al. concluded that security work is collaborative both within organizations and distributed across the Internet. Our study provides a broader scope on the collaborative nature of security work, with 21 interviews of security practitioners involved not only in intrusion detection, but also other security related activities within the organizations.

METHODOLOGY

This study is part of an ongoing project that aims at proposing guidelines to evaluate and devise tools used for managing IT security. For investigating the theme of interactions between security practitioners and other stakeholders, three research questions framed our study:

- When and how do IT security practitioners interact with other stakeholders?
- Which tools do they need to interact effectively?
- What factors are behind miscommunications?

Data collection

Collecting data on how organizations manage IT security poses several challenges [15]. For example, practitioners do not have time to participate, they are not willing to disclose security information, and their contact information is not publicly available. To address these challenges we used two main strategies. The first was the use of professional contacts of the research team. The second strategy was a graduated recruitment approach. Potential participants were asked only to answer a short questionnaire that had a final question asking if the participant was willing to give a one-hour interview.

We collected 21 semi-structured interviews of IT security professionals for the analysis presented in this paper. As another source of data, we also collected data on the development of policies from participatory observations in one post secondary organization in Canada.

Questionnaires and Semi-Structured Interviews

We obtained 30 questionnaires and 21 interviews of IT professionals with security responsibilities from HOT Admin's fieldwork. The questionnaire had two objectives: first, to obtain demographic information about our participants. Second, to invite participants to to be interviewed.

Semi-structured interviews covered different aspects of IT security. Our participants answered questions about their tasks, the tools they used, and the communications they had to perform to do their job. To reduce the interviewer's bias and obtain information from different perspectives during the interviews, each interview was performed by a team of two researchers. This team approach allowed interviewers to ensure coverage of interview questions and to probe for details from different angles for those answers that contained relevant data.

Participatory observation

We used an ethnographic approach [7] to collect more data about the different roles and communications performed by security practitioners in real settings. This ethnographic approach consisted of participatory observation which is underway at one post-secondary educational organization centre in Canada. The observer had spent 60 hours working under the supervision of a senior IT security professional. The main task of the observer has been the development of policies; he has participated in eight meetings to date with IT specialists to write and update a set of internal policies with respect to data classification, secure browsing, and use of remote connections. Although preliminary, the results of this participatory observation were used to cross-validate and complement our findings from the analysis of interviews.

Data analysis

The semi-structured interviews' data were analyzed using grounded theory [5]. The first step was to identify in the interviews when participants described how they had to interact to perform a task. These situations were coded iteratively, starting with open coding and continuing with axial and theoretical coding [5]. At this stage, results were organized in three categories. The first one comprised a list of different situations or contexts our participants described they had to interact with other stakeholders to perform their security related tasks. The second one accounted for tools and resources (skills and knowledge) participants mentioned as necessary to interact. The third summarized the sources of errors identified by participants when communicating with other stakeholders.

The posterior analysis on the interviews was based on further elaboration of the "memos" [5] written during the coding process for each part of the analysis. For the overall project, four researchers performed the analysis process, each one focusing his or her analysis on different themes. In particular, the theme about interactions was analyzed by one researcher but it had a considerable degree of overlap with other themes analyzed by other researchers (e.g. tasks performed by security practitioners, errors made in security related tasks). This overlap made triangulation possible at a researcher level.

Profile of our participants

Table 1. Jobs descriptions of our participants

Position	Academia	Industry
IT Managers	P1, P15, P17, P18	P16
IT systems specialists	P6, P7, P8, P10, P14	P12, P13, P19
IT security specialists	P2, P3, P4, P9, P11	P5, P20, P21, P22

Fifteen of our participants (70%) came from post-secondary organizations and six (30%) from five different commercial organizations (financial services, insurance, consultant, non-profit organizations and manufacturing (2)). The profile of our participants is shown in table **??**

Thirteen of our participants provided information through the questionnaire about the time spent on security tasks. On average, those thirteen participants devoted almost 35% of their time on IT security responsibilities. There was, however, a broad range of time spent on IT security tasks, with two spending more than 75%, whereas each of the two IT managers spent less than 10%.

RESULTS

We identified in our participant's interviews several stories of high-level activities in which IT security-related communications occur. After describing these activities and communications, we continue by presenting the tools used to interact and the sources of communication-related errors. To further illustrate our findings, our results conclude with specific descriptions of the interactions, tools, and miscommunications during two of the activities: *responses to security incidents* and *development of policies.*

It is important to note that, due to the nature of semi-structured interviews, not all topics were discussed at the same level of detail with all participants.

Interactions With Other Stakeholders

We identified eight types of activity where participants had to interact with other stakeholders. These different interactions represented a challenge for our participants, who required different strategies to communicate security issues to stakeholders with different backgrounds and interests. Table 2 shows the eight activities described by our participants as well as a summary of stakeolder's interactions for each activity.

One of the most important skills required by our participants to interact were *good communications.* Several aspects of good communication were described by participants, for example: openness, availability and accessibility. These aspects were necessary in order to both educate other stakeholders in terms of IT security and to make security practices more effective.

To perform security tasks our participants had to coordinate, collaborate, and cooperate with other stakeholders (definitions of coordination, cooperation and collaboration as shown in [18]). Although these three types of interactions were combined, some tasks were characterized by a bigger influence of one or two of them. For example, participants mainly coordinated time and resources with other stakeholders to perform security audits. We will briefly describe each activity, giving a sense of each.

The objective of *security audits* was to find vulnerabilities in the IT infrastructure and generate reports with recommendations for other IT specialists. These checks on the infrastructure could be in the context of formal audits performed either by internal departments or by external audit companies, or as part of less formal internal checks within the IT department. When our participants performed the audits, they had to interact with other IT specialists to communicate and explain the vulnerabilities found on the systems. In other cases, they provided support and interacted actively with the IT specialists to cope with recommendations given by the auditor.

For *designing services incorporating security criteria*, our participants assumed the role of consultants. On one hand, they had to plan with other specialists the deployment of new services, such as VPN SSL remote access, integrated solution for collaborative environments, and internal customized services. On the other hand, they had to participate in committees to approve new projects or changes in the infrastructure, checking how security criteria were incorporated in the changes. Typical issues that our participants needed to address as consultants were: where access controls should be, what types of antivirus protection, how to implement services when there were firewalls in the middle, which firewalls could be supported by the existing infrastructure, and which security vendors or providers to choose. For the last point, our participants needed to interact with potential vendors involved in the project, in order to ask for specifications or evaluate security features of the products offered.

To *solve end-user IT security issues*, our participants usually received notifications from automated incident monitoring systems.Depending on the type of request, they had to either get more information from the users or visit them to check *in situ* their computers. One of the organizations in our sample did not have a centralized monitoring system, so the communications between the specialists and users were directly performed by phone or e-mail.

To *implement access security controls*, it was necessary to interact with other departments, such as Human Resources. These interactions were motivated by the lack of a consolidated database of employees and active users on the systems. For example, one of our participants had to coordinate with Human Resources to verify the list of active users in their Active Directory systems.

Our participants had also to *train and educate other specialists* on security issues in a variety of circumstances, such as training new employees in the organization's privacy procedures.

When the organization had distributed responsibilities in terms of the IT infrastructure, the *notification of new vulnerabilities* announced by IT providers or other security entities also triggered interactions among our participants. In these cases, they forwarded the information to other specialists, both as notification, and also to confirm with them.

The remaining two activities are described briefly now, but will be presented in full as illustrative examples of interactions, tools, and sources of errors. To *respond to security incidents*, our participants needed to actively interact with other stakeholders. One example of such an interaction was verifying the reasons for peaks of e-mails or traffic in highly distributed environment. In such cases, our participants needed to correlate with sources of information that were managed by other IT specialists to find out the physical location of the affected devices. The *development of policies* generally involves committees with different IT specialists, managers and top executives from the areas affected by the policy.

These eight activities described by our participants indicate the diversity of IT security-related activities. They also emphasize the importance of interactions to perform the tasks. Furthermore, the scenarios themselves speak to the need for intimate knowledge of the organization in order to involve stakeholders from pertinent areas.

Tools used to interact with other stakeholders

Participants used multiple communication channels, such as e-mail, text and video chat, phone, and meetings. These channels were used, for example, to broadcast information, receive notifications, share documents, gather information, send requirements, and report about security issues.

Our participants all relied heavily on e-mail. They reported using e-mail to broadcast information to other IT specialists and share documentation. E-mail was also reported to be easier to track and read from home than other solutions, like ticketing systems (P3 and P15). Nevertheless, their perceptions about the effectiveness of e-mail varied. For example, P4 claimed that misunderstandings arise easily through the casual language common in many e-mails and expressed the need for care about how things were written. This participant compared e-mail unfavorably with verbal communication in situations that required clarification of some topic. However, P3 and P5 thought e-mail was useful to formalize and clarify what they had discussed during

Table 2. Types of activity in which IT-security communication occurs.

Activity	Occurrences	Stakeholders involved
Perform and respond to security audits on the IT infrastructure	P2, P4, P5, P16, P21	1. Coordinate or collaborate with IT specialists 2. Coordinate with auditors
Design and revise security services or projects	P2, P11, P14, P15, P17	1. Coordinate and collaborate with other IT specialists 2. Coordinate and collaborate with organization's multidisciplinary committees 3. Coordinate with vendors of security technology
Solve IT security issues of end users	P3, P10, P15, P20	1. Cooperate and collaborate with IT specialists 2. Cooperate with external specialists (from the organization) 3. Coordinate with end users
Implement security controls	P4, P5, P20	1. Cooperate with other IT specialists 2. Coordinate with other departments: Human Resources
Educate and train other employees	P5, P15, P16	1. Cooperate with IT specialists 2. Cooperate with managers/executives 3. Cooperate with end users
Mitigate new vulnerabilities	P2, P9	1. Cooperate with other IT specialists 2. Coordinate with vendors of security technology 3. Cooperate with external IT security entities
Respond to security incidents	P1, P2, P3, P4, P5, P7, P9, P11, P12, P13, P15, P17, P18	1. Coordinate and cooperate with Other IT specialists 2. Coordinate and cooperate with specialists from legal department 3. Coordinate and cooperate with external specialists (from the organization) 4. Coordinate with vendors of security technology
Develop security policies	P1, P2, P21	1. Coordinate and collaborate with other IT specialists 2. Coordinate with end users 3. Coordinate and collaborate with managers/executives

meetings.

The large quantity of e-mails was reported to be an issue. However, P9 was able to troubleshoot at a glance by noting the number of new e-mails in certain folders (the more e-mails from specific systems, the more likely a problem was occurring).

Keeping record of communications was important for participants. P20 was careful to keep two CD-ROM copies of all e-mail. In the case of access control administration, if only logged-in users can use the e-mail system, an e-mail reply from an authorized person is taken as proof of authorization for access.

Besides e-mail, a few participants used other tools like text or video chat to communicate. Again, the perceptions of the usefulness varied. P9 and P11 found chat a good tool for getting an immediate response and asking about specific information (e.g., a system's command syntax), while P8 and P11 found it distracting with no guarantee of response. Video chat was preferred because it complemented the advantages of chat with images. However, P9 commented that some colleagues did not use video chat because they found it unnatural, with shifts between what is seen and what is said, and with each party not seeing the eyes of the other.

Five participants (P1, P8, P11, P14, P15) stated they preferred to use verbal communication (e.g. face-to-face or phone) when they had to interact with other stakeholders. Face-to-face communications allowed them to quickly interact and avoid misunderstandings.

Internal web sites were used to keep track of meetings (P2). These sites were also used to show information to end-users about their IT security services. For example, in order to reduce the overhead of questions from end-users, P10 employed an internal web site to show users the status of their spam filters.

Another common communication system mentioned by our participants (P1, P3, P20) was an incident tracking system (used by the helpdesk). This type of system automatically generated tickets and send them to IT specialists when users reported a problem about the IT infrastructure. The tickets were assigned depending on the complexity and type of the incident. The initial assignment was based on the information the helpdesk received from the users. If the first level of specialists who solved recurrent IT issues could not solve the problem, the ticket was re-assigned to other specialists with more security expertise.

Interactions with different stakeholders made reporting an important feature of security tools. Our participants mentioned tools like Nessus (P9, P12, P21) (used to show the vulnerabilities of the IT infrastructure), and McAffe ePolicy Orchestrator (EPO) (P3, P4, P14) (used to summarize the virus activity of the systems). P9, who coordinated with other IT specialists the mitigation of vulnerabilities, explained the flexibility of Nessus' reports in terms of how easy it was to browse through their links and check the vulnerabilities at appropriate levels of detail. This flexibility allowed him to have a general overview of the vulnerabilities, whereas other specialists could have a detailed view of the information to mitigate the vulnerabilities. McAffe EPO was used to track the activity of malicious software in users' systems.

Our participants also mentioned other reporting features that security tools should include. For example, security tools should generate reports showing to other stakeholders the economic benefits of applying security controls (P3), reports should specify what is "normal" traffic in the network and what is not, based on long time correlation features (P3), and reports should help security practitioners to prioritize their activities, showing high level risks and compliance of the IT infrastructure with patches, antivirus and countermeasures for new vulnerabilities (P4)

Sources of errors

The importance of effective interactions to perform security related tasks makes it necessary to understand the problems during communications and their consequences. Several types of miscommunications emerged from the interviews, including not following preestablished procedures, not sharing the same perception of risk, the lack of timely communications, and language barriers.

Not following change management procedures generated communications overhead and impacted productivity. P2 highlighted the consequences of not integrating security with other activities such as the design of new projects and day-to-day operations. When this integration did not exist and security was incorporated as an add-on at the end of the day, security specialists needed much more information and communication with the other areas to understand and apply security criteria to the new systems.

Another type of miscommunication happened when our participants had to interact with stakeholders that did *not share the same perception of security risks* (e.g., business people). In these circumstances, some participants (P5 and P14) assumed the role of "risk evaluator", explaining the risks associated with the requirement to the "risk taker". By doing so, our participants tried to reach a common understanding of the situation in terms of levels of risk.

Lack of timely communications was another issue mentioned by our participants. For example, high workloads interfered with communication; our participants had no time to notify involved parties of changes during quick responses to incidents. Similarly, given the complexity of the IT infrastructure, IT specialists might not anticipate the consequences of local changes in other network domains, and thereby consider it unnecessary to inform other parties about reconfiguration of systems. Lack of timely communications with vendors was also mentioned.

Language barriers was another cause of miscommunications. One of our participants (P4) had to interact with an IT specialist from Germany to disable a phishing server. Another participant (P10), who spoke English as a second language (ESL), described how he misunderstood a question from his boss because of the language. As a consequence, our participant gave wrong information about the consequences of an incident that had affected the access to the networks.

Avoiding Misunderstandings

Our participants had to be very careful with the tone of the requirements they made (P9, P2, P21). Interactions related to the adoption of new security controls had to be performed carefully to optimize their effectiveness; people had to understand the goals of the security controls without feeling that they had to follow blindly orders from the IT security group. In the same vein, our participants had to trade between effectiveness and attractiveness of the news they spread within the organization. They had to minimize as much as possible what was necessary to communicate without giving the impression that security information was too simple or unimportant.

Our subjects also mentioned some countermeasures to avoid miscommunications. For example, the use of the need-to-know principle [26] to communicate security matters was mentioned to avoid misinterpretations by stakeholders not directly involved in investigations involving violations of internal policies. Other countermeasures included education and training about risks within the organization and proactive communications to keep other parties informed about reconfigurations in the systems.

Another way to avoid misunderstandings was the use of face-to-face communications. This type of communication allowed our participants to communicate more information and give more context. However, our participants were also concerned about recovering the content of face-to-face or phone communications. For example, one participant (P5) had troubles justifying an account he had enabled in a system. This participant had received the requirement by phone, and did not have a written record of it when the system was audited.

ILLUSTRATIVE EXAMPLES

To illustrate interactions, use of resources, and the role of misunderstandings, we next describe with more detail two activities performed by our participants: *respond to security incidents* and *development of policies.*

Interactions in responding to security incidents

Responding to security incidents was the most commonly mentioned activity by our interviewed participants. Interactions during security incidents were complex, involving collaboration, coordination, and cooperation. Other particular characteristics of interactions during security incidents were the use of multiple communication channels and good communication skills to share knowledge between different specialists during the investigation.

Depending on the incident, communication channels during the analysis often had to be combined. One participant (P15) described how during an incident that compromised the performance of the whole network, communications included e-mails to notify people about the incident and share general information, as well as phone and face-to-face communications to be sure they had the same understanding of the situation.

When the causes of the incident were not evident, participants found it useful to interact with specialists that were new in the investigation or had a different background. One of the stories we collected exemplified this finding: one practitioner (P13) had to investigate an incident where the monitoring system only reported that the systems were down (he was using SmokePing as a monitoring tool). He decided to check *in situ* the systems by asking help from another specialist *"because two eyes are better than one"*. Based on their previous experiences and on the fact that the hardware looked normal (panel alarms and cable), they developed the hypothesis that the problem was in the devices that controlled the upstream traffic of the network. At this point, they decided to involve another specialist in the analysis. She thought that the problem was with a small switch that was not being monitored and had not been checked during the previous inspection; they reset the switch and the network recovered from its failure. Similarly, another participant (P11) described needing cooperation from another department's specialist to trace the flow of traffic in a network which was having low performance. As a result of this collaboration, they were able to isolate the device that was making the outbound traffic slower.

Large scale incidents due to malicious software represented an interesting type of incident where dynamically formed ad-hoc groups were required for response. As an example, a participant (P4) described how he had to coordinate, as the "owner" of an incident, the activities of such a group. Their main objective was to clean the MS Windows machines of the IT infrastructure that had been infected by a virus. The ad-hoc group was formed by approximately 20 people, most of them network and MS Windows specialists. They were organized in two layers: the first layer was in charge of evaluating the damage in terms of services affected. The other group had to analyze the malicious software and generate a plan to patch the infected machines.

Another type of interaction occurred during the investigation of suspected violations of internal policies. These investigations were characterized by the specific descriptions of the communication channels used to exchange information. Examples of these characteristics were: 1) the initial requirements to investigate usually did not follow the formal channels to start the investigation of incidents (use of "back-channels"), 2) security practitioners required formal and written evidence of the requirements to access personal data of the employees, and 3) they needed to interact with the employees of the legal department.

Our participants also interacted with external specialists who had more experience or had had similar problems. One example was given by a participant (P13) who was trying to find the cause of one suspected security incident: *"So we are at that stage where we are trying to track down, you know looking through the archives of that mailing list to see if anyone else has had similar problems."* Another example of external interactions happened during a phishing attack. This participant (P4) had to coordinate with an administrator in Germany to take down a phishing web site. In this case, *"the biggest challenge was the language barrier"*, he said.

As previously described, misunderstandings such as lack of communication can also be cause of security incidents. Another participant (P3) described the overhead of not only keeping track of all the communications during the investigation of incidents, but also sending clarification questions through e-mail to other stakeholders to avoid misunderstandings.

Development of policies

Developing security policies made intensive use of interactions. As in security incidents, participants had to use multiple communication channels to interact with other stakeholders and get feedback from managers. The intensive use of tacit knowledge about the organization and threat analysis were other interesting characteristics that make developing policies interesting from the point of view of interactions.

During participatory observation, we observed how security and IT specialists developed policies, use an internal web site accessible by everyone as the main repository for the drafts, and related documents used during the policy writing process. E-mail was also used to share related documents with the whole group. Threat analysis was necessary in order to cover all possible circumstances in which the policy should apply. In other words, threat analysis allowed our participants to map different risks with the text in the policy.

Our observations also uncovered some issues that did not emerge from the interviews. One of these issues was related to the tacit knowledge within the organization required to write the policies. Tacit knowledge was required to devise "usable" policies, in terms of matching security principles with the tasks of different stakeholders. IT professionals involved in writing the policies knew well the jobs performed by different stakeholders, the common tasks they performed, and the resources they utilized. For example, our participants had to know how different specialists made use of the information on the servers, before imposing restrictions on the use of that information.

Another issue uncovered doing participatory observation was related to the knowledge of IT security tools. Our participants required a deep knowledge of what general IT and security tools could do to implement the principles stated in the policies. IT specialists involved in the process had to go back and forth, refining the policy text, considering how tools were able to support the implementation of the controls stated in the policies. For example, for a policy related to data protection, the requirements about encryption of critical data made it necessary to study how different encryption tools could be adapted to the organization' needs. This process not only elongated the writing of the policy, but also confirmed Botta et al.'s general finding of the importance of documentation for IT security professionals [3].

As mentioned before, participants tried to avoid misunderstandings with managers by asking continually for their feedback on, for example, the topics covered by the policies. Misunderstandings happened within the group that developed the policies. For example, despite the fact that the format of the policies was agreed at the beginning of the writing process, some participants wrote their policies using different formats, thinking that the new formats would communicate better the contents of the policies. These differences added overhead to the policy development process.

DISCUSSION

In most of the participant's organizations, IT security related tasks require interaction between a variety of different stakeholders. Knapp et al. [13] also expressed this characteristic of IT security. Furthermore, our results show that IT security practitioners exhibit significant diversity, as indicated by the variety of high-level tasks that contextualize their interactions. To perform these tasks, our participants needed to interact with other stakeholders to share knowledge, to work on assets they did not manage, and to solve security issues of end-users. Participants also required good communication skills to perform their jobs.

Interdependency and diversity made interactions complex for our participants. The next section elaborates on the complexity of security related communications.

Complexity of Interactions

During interactions, our participants had constantly to persuade other stakeholders about the importance of security controls. In this process, communication style was important in order to approach stakeholders that did not share the same perception of risks. For example, one participant (P22) expressed the need for diplomacy to achieve cooperation.

Koskosas and Paul [14] studied how risks are communicated in financial organizations. They concluded, that risk communication "plays a significant role at the macro-goal level of security management," and affects the setting of banking security goals. Our analysis provided more empirical evidence over a wider range of organizations on the importance of communicating risks for security practitioners. We showed how security practitioners assume the role of "risk evaluators" during interactions with other stakeholders.

Good communication skills were necessary to adapt interactions to the context of the activity. Our participants had to be proactive to perform audits, design new services, implement security controls, educate and train, and develop policies. They had to be reactive to solve IT security issues from end users, manage new vulnerabilities, and respond to incidents.

Tacit knowledge was also prominent during interactions related to IT security activities. For example, in order to write policies our participants had to know about other stakeholders' tasks and how security controls would be integrated to those tasks; to respond to incidents they knew which specialist had to be involved in the investigation; to integrate security with new IT services, they had to know about the services the organization provided. Altogether, this suggests that practitioners of IT security tend to be centers of "transactive memory" [24, 19]. Kesh and Ratnasingam [12] highlighted the need of transforming tacit security knowledge into explicit knowledge. There is some debate as to wether or not such a thing is feasible [21], or desirable (why should they give away their stock in trade?). Our participants transformed or coded their tacit knowledge into (1) implementations such as policy and its interpretation in terms of technology; (2) statements of evaluation, when playing the role of "risk evaluator"; and (3) development of programs for the training of other specialists.

Our participants had to transform knowledge to perform their tasks. For example, to develop policies they had constantly to convert knowledge between tacit and explicit forms. Using Marwick's analysis of technologies used for organizational knowledge creation [17], the process of developing policies can be separated in the following steps: first, to find templates about policies on the Internet, using a browser and a searching engine (explicit to explicit knowledge). Second, read other organizations' policies and interpret their meaning (explicit to tacit knowledge). Third, to adapt the templates and the information found using tacit knowledge of the organization, having internal meetings where experiences on security issues are commented (tacit to tacit knowledge. Fourth, to disseminate the policies presenting the policies in meetings and internal web sites (tacit to explicit).

We found that sources of breakdown of IT security interaction belong to information errors according to Hinckley's classification ([10] cited by [4]). More specifically, as indicated in Kraemer and Carayon's framework [16], heavy workload and lack of formal communications can be classified as belonging either to the organization, or to the task. We also found how ineffective interactions can be the source of security incidents or increase the levels of risk. For example, a lack of communications when making changes in firewalls can cause connection problems for other users of the network. Also, a lack of timely response from a vendor about new patches exposes the IT infrastructure to attacks.

SUPPORTING INTERACTIONS WITH TOOLS

The need for better support for collaboration in security tools has been recognized previously. Goodall et al. [8] report on the need for security tools as intrusion detections systems to support the collaborative nature of detecting intrusions. Chiasson et al. [6] mention how security interfaces should facilitate interaction within the security community. Our analysis showed how our participants have to use communication channels that were not integrated with their security tools and did not always cover all their needs. For example, on the one side, they needed to avoid the possibility of misunderstandings during communications. On the other side, they needed to keep track of agreements for future audits. Keeping tracks of agreements was linked to the need of archiving communications.

There are opportunities for tools to cut down the complexity of interactions that security practitioners have to face within organizations. For example, security practitioners need better reporting features to interpret the information from different communication channels. One participant desired reporting tools that compare abnormal traffic against normal traffic from systems or from users behavior. In the same vein, reporting tools should indicate the levels of risk in the IT infrastructure—specifying compliance with patches, antivirus and countermeasures for new vulnerabilities. This last characteristic might help security practitioners to prioritize their tasks.

Security practitioners also need support to disseminate their knowledge. They have to make trade offs between the need for pushing their knowledge about IT security to other stakeholders, and the various priorities that different stakeholders may have. We identified the development of security policies as one way to push security knowledge to the rest of the organization, mixing explicit knowledge about good security practices with tacit knowledge that security practitioners use to adapt policies to the organization reality. Marwick's revision on the use of technologies for knowledge management also highlights the need of better tools to transform tacit knowledge into explicit knowledge [17]. In the case of security, the effectiveness of this dissemination process may be difficult to measure, as it is related with the improvement of security level of the organization.

There also particularities in the way security practitioners need to disseminate their knowledge. Botta et al. [3] identify the need for *flexible reporting* to support some security-related tasks. Our current analysis indicates that flexible reporting can be broken down into the following characteristics: On-line and automatic generation of different reports for different stakeholders and the use of different layers of information (general vs. specific). This last requirement confirms Chiasson et al.'s [6] proposal of using ecological interfaces to design security systems, showing security information in 5-levels of abstraction, with different levels of details depending on the user.

Reporting in security systems also has to consider specific constraints related to communicating IT security issues. One of these constraints is the employment of the security principle of *need to know*. This constraint on communication was also mentioned by Haber and Kandogan but as a characteristic of IT security administration [9]. Our analysis showed that *need to know* principle is used to both respect confidentiality of information related to investigation of violations of internal policies and to reduce the potential for miscommunication by reducing communication to those stakeholders without enough background on security issues. Flexible reporting incorporating specific security constraints is a field where developers can improve communication features of security tools (or *vise versa*).

In addition to using the *need to know* principle to avoid errors during interaction, our participants also used checklists, proactive communications, and training. These strategies may also provide opportunities for tool development. For example, firewall management systems could have a checklist of stakeholders who are automatically informed about configuration and other changes. Each stakeholder could respectively receive the information at the appropriate level of detail, language, and channel (e-mail, text message, web site).

Finally, tools may be used to reduce communication overhead. For example, one of our participants used an embedded feature of a spam filter tool to publish on a web page the status of users' e-mails. This way, he avoided questions from the users about what happened with their e-mails when a new spam rule was added. We think this is another opportunity for improving communication support in security tools.

CONCLUSION

Our results include factors behind the distribution nature of IT security, a list of activities where IT security people have to interact with stakeholders, the tools employed, and the sources of errors during interactions. We provided new insight into strategies used to interact and make more effective the response to security incidents and the development of policies. We also identified typical sources of errors and countermeasures during interactions.

Our theory shows the complex environment where security practitioners not only to perform security specific tasks, but also interact with stakeholders with different backgrounds and needs. This makes it difficult to disseminate security knowledge. Tools used by security practitioners do not provide enough support for this highly interactive environment. Tools need to be integrated with the use of different communication channels and the particularities that security communications impose.

We have only begun to answer questions on the complexity of interactions performed by security practitioners. We need more empirical data, such as contextual interviews, to further understand the role of security practitioners within their organizations. This future research will expand and refine our understanding of the interactions with respect to different kinds of contexts.

REFERENCES

1. K. Beznosov and O. Beznosova. On the imbalance of the security problem space and its expected consequences. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, pages 128 — 140, Plymouth, UK, July 10 2007.
2. F. J. Björck. *Discovering Information Security Management.* Doctoral thesis, Stockholm University, Royal Institute of Technology, 2005.
3. D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding IT security professionals and their tools. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 100–111, Pittsburgh, Pennsylvania, July 18-20 2007.
4. L. P. Chao and K. Ishii. Design error classification and knowledge management. *Journal of Knowledge Management Practice*, 5, 2004.
5. K. Charmaz. *Constructing Grounded Theory.* SAGE publications, 2006.
6. S. Chiasson, P. C. van Oorschot, and R. Biddle. Even experts deserve usable security: Design guidelines for security management systems. presented at the SOUPS Workshop on Usable IT Security Management (USM), July 18 2007.
7. D. M. Fetterman. *Ethnography: Step by Step.* Sage Publications Inc., 1998.
8. J. R. Goodall, W. G. Lutters, and A. Komlodi. I know my network: Collaboration and expertise in intrusion detection. In *CSCW*, volume 6390, Chicago, Illinois, USA, November 6 — 10 2004.
9. E. M. Haber and E. Kandogan. Security administrators: A breed apart. presented at the SOUPS Workshop on Usable IT Security Management (USM), July 18 2007.
10. C. Hinckley. *Make No Mistake.* Productivity Press, Portland, OR., 2001.
11. E. Kandogan and E. M. Haber. Security administration tools and practices. In L. F. Cranor and S. Garfinkel, editors, *Security and Usability: Designing Secure Systems that People Can Use*, chapter 18, pages 357–378. O'Reilly Media, Inc., Sebastapol, 2005.
12. S. Kesh and P. Ratnasingam. A knowledge architecture for IT security. *Commun. ACM*, 50(7):103–108, 2007.
13. K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford. Managerial dimensions in information security: A theoretical model of organizational effectiveness. https://www.isc2.org/download/auburn_study2005.pdf, 2005.
14. I. V. Koskosas and R. J. Paul. The interrelationship and effect of culture and risk communication in setting internet banking security goals. In *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 341–350, New York, NY, USA, 2004. ACM Press.
15. A. G. Kotulic and J. G. Clark. Why there aren't more information security research studies. *Information & Management*, 41(5):597–607, 2004.

16. S. Kraemer and P. Carayon. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38:143–154, 2007.

17. A. D. Marwick. Knowledge management technology. *IBM Systems Journal*, 40(4):814–830, 2001.

18. P. W. Matessich and B. R. Monsey. *Collaboration: what makes it work. A review of research literature on factors influencing successful collaboration.* Amherst H. Wilder Foundation, St. Paul, MN, 1992.

19. Mohammed, S. and Dumville, B. Team mental models in a team knowledge framework: Expanding theory and measurement across disciplinary boundaries. *Journal of Organizational Behavior*, 22(2):89–106, mar 2001.

20. H. Qeensland Government, S. I. Recording, and Notification. Incident definition. http://education.qld.gov.au/strategic/eppr/health/hlspr005/definitions.html, 2007.

21. K. Schmidt. Of maps and scripts—the status of formal constructs in cooperative work. In *Proceedings of the international ACM SIGGROUP conference on Supporting group work: the integration challenge*, pages 138–147, Phoenix, Arizona, United States, November 1997.

22. E. A. Smith. The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, 5(4):311–321, 2001.

23. F. O. Sveen, J. Sarriegi, E. Rich, and J. Gonzalez. Toward viable information security reporting systems. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2007)*, pages 114–127, 2007.

24. D. M. Wegner. *Transactive memory: A contemporary analysis of the group mind.* In M. B. & G. G. R. (Eds.), Theories of Group Behavior, 1986.

25. K. E. Weick and K. M. Sutcliffe. *Managing the Unexpected.* Jossey-Bass, 350 Sansome St., San Francisco, CA 94104-1342, 2001.

26. I. S. W. P. West Virginia University. need-to-know principle definition. http://infosecurity.wvu.edu/policy/glossary.html, 2007.