Security Practitioners in Context: Their Activities and Interactions

Rodrigo Werlinger
University of British Columbia.
Vancouver, Canada
rodrigow@ece.ubc.ca

Kirstie Hawkey
University of British Columbia.
Vancouver, Canada
hawkey@ece.ubc.ca

Konstantin Beznosov
University of British Columbia.
Vancouver, Canada
beznosov@ece.ubc.ca

CHI 2008, April 5 – April 10, 2008, Florence, Italy
ACM 978-1-60558-012-8/08/04.

Abstract
This study develops the context of interactions of IT security practitioners. Preliminary qualitative analysis of 22 interviews (to date) and participatory observation has identified eight different types of activities that require interactions between security practitioners and different stakeholders. Our analysis shows that the tools used by our participants do not provide sufficient support for their complex security tasks, including the interactions with other stakeholders. We provide recommendations to improve tool support for security practitioners.

Keywords
Security Tools, Usable Security, Qualitative Analysis

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

Introduction
Information security has become a critical issue for organizations. Security practitioners work in a distributed, interdependent, and collaborative environment [1], where communication breakdowns may lead to security vulnerabilities. Kandogan and Haber [4] find that "security administration requires collaboration between people at many levels," and suggest that IT tools should improve their support for collaboration and information-sharing tasks performed by security practitioners [5]. Furthermore, Knapp et al.

Position	Participant
Academia	
IT Manager	P1, P15, P17, P18
IT Systems Specialist	P6, P7, P8, P10, P14
IT Security Specialist	P2, P3, P9, P11
Industry	
IT Manager	P16
IT Systems Specialist	P12, P13, P19
IT Security Specialist	P4, P5, P20, P21, P22

Table 1: Profiles of our participants. Thirteen came from academia and nine from industry (financial services (2), insurance, non-profit organization, research institutions (2), manufacturing (2), and security consultant).

[6] identify the high level of interdependency of security tasks. However, these studies do not provide details on how security practitioners interact and communicate with other stakeholders, or how these interactions vary depending on the security activity being performed. This current lack of a rich understanding of IT security management makes it difficult for HCI researchers and security tool developers to improve security and communication tools [1, 3], and to develop tests to measure the usability of security tools in real, complex scenarios [7].

The study presented in this paper is one research theme of an ongoing research project, HOT Admin. In an effort to develop better IT security tools, this project aims to address the above limitations by investigating how human, organizational, and technological factors interplay (preliminary results of this project published in [1]). The contribution of this paper is twofold. First, we analyze the interdependency of IT security tasks by showing the different roles, communications, and resources used by IT security professionals in real contexts. Second, we identify opportunities to improve tools used by security professionals to collaborate, cooperate, and coordinate with other stakeholders in order to effectively perform their tasks. We next present the design of our qualitative study. We then show our results, which describe interactions in context. Our discussion provides recommendations for improving security tools.

Methodology

Our goal was to develop a better understanding of how communication and security tools support interactions between security practitioners and other stakeholders. Our research questions were: (1) When do security practitioners interact with other stakeholders? (2) What tools do they use to interact? and (3) How can we improve these tools? To answer these questions, we needed empirical data about security practitioners working in real environments. We used qualitative methods to obtain and analyze these data.

Data Collection: The field study has provided us with three sources of data: questionnaires, interviews, and participatory observation. The questionnaire provided demographic information about our participants. We conducted 34 in-situ semi-structured interviews from IT professionals with security responsibilities (22 have been analyzed to date). The profiles of our participants are shown in Table 1. The interviews covered various aspects of IT security (tasks, tools, and communications). 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. Another source of data came from participatory observations by the first author in one organization. To date, the observer has worked over 75 hours under the supervision of a senior IT security professional.

Data Analysis: We first identified instances in the interviews when participants described interacting to perform a task. These situations were coded iteratively, starting with open coding and continuing with axial and theoretical coding. Results were then organized by the different activities, which provided context for the interaction and the tools necessary for interaction. Posterior analysis was based on further elaboration of "memos" written during the coding process. For the overall project, four researchers performed the analysis process, with each focusing their analysis on different themes. The interactions theme was analyzed by the first author but had a considerable degree of overlap with other themes (e.g., tasks performed by security practitioners). This overlap made triangulation of analysis possible at the researcher level.

Analyzing Interactions in Context

We have identified to date eight types of activities where participants had to interact with other stakeholders. These interactions represented a challenge for our participants; they required different strategies to communicate security issues to

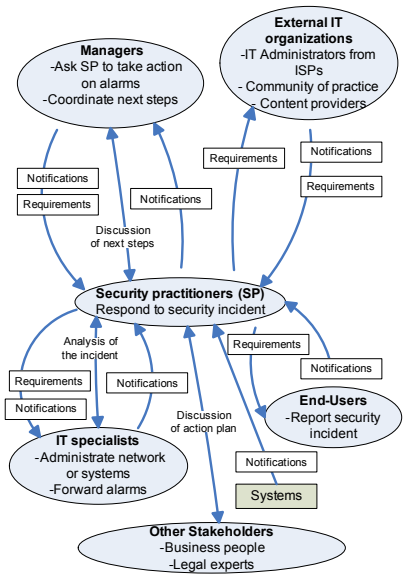

Figure 1: Example of interactions and types of information exchanged during the response to a security incident. Bidirectional arrows indicate face-to-face interactions.

stakeholders with different backgrounds and interests. We give a brief description of each activity type.

P*erform security audits.* Participants (P2, P4, P5, P16, P21, P22) had to find vulnerabilities in the IT infrastructure and generate reports with recommendations for other IT specialists. When our participants performed the audits, they had to interact with other IT specialists to communicate and explain the vulnerabilities found in the systems. In other cases, they interacted actively with IT specialists to respond to recommendations provided by auditors.

Design services incorporating security criteria. Participants (P2, P11, P14, P15, P17, P22) assumed the role of consultants. On the one hand, they had to plan the deployment of new services with other specialists, such as remote access 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.

Solve end-user IT security issues. Participants (P3, P10, P15, P20) usually received notifications from automated incident monitoring systems, or directly from end-users. 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.

Implement access security controls. Participants (P4, P5, P20) found it necessary to interact with other departments, such as Human Resources (HR), to implement new user accounts. These interactions were due to the lack of a consolidated database of employees and active users of the systems.

Train and educate other specialists. Participants (P5, P15, P16, P22) had to educate and train other stakeholders on security issues. For example, they had to train new employees on the organization's privacy policies and procedures.

Analyze new vulnerabilities. When the organization had distributed responsibilities across the IT infrastructure, new vulnerabilities announced by system vendors or security entities triggered interactions among IT professionals (P2, P9). Participants analyzed and forwarded the information to other specialists, both as notification, and also to confirm the vulnerability.

Develop policies. Participants (P1, P2, P21, P22) took part on committees with IT specialists, managers, and executives from the organization's areas affected.

Respond to security incidents. Our participants (P1, P2, P3, P4, P5, P7, P9, P11, P12, P13, P15, P17, P18) needed to actively interact with other stakeholders during the response to security incidents (figure 1 summarizes these interactions). This figure also gives a sense of the type of information required by the different stakeholders involved in security related activities.

Tools Used during Interactions

Participants used multiple communication channels to interact, such as e-mail, text and video chat, phone calls, and meetings. These channels were used to broadcast information, receive notifications, share documents, gather information, send requirements, and report security issues. Our participants all relied heavily on e-mail. They reported using e-mail to broadcast information to other IT specialists and share documents. E-mail was also reported to be easier to track and read from home than other solutions, such as ticketing systems (P3 and P15). Nevertheless, their perceptions about the effectiveness of e-mail varied. P4 claimed that misunderstandings arise easily through the casual language used in e-mails and expressed the need for care about how things were written. P4 also preferred verbal communication over e-mail in situations that required clarification. In contrast, P3 and P5 thought e-mail was useful to formalize and clarify what they had discussed during meetings. The large quantity of e-mails from both systems and people was

reported to be an issue. However, P9 was able to detect anomalies in the systems by noting the number of new e-mails in certain folders (the more e-mails from specific systems, the more likely a problem existed).

Keeping a record of communications was important for participants. P20 was careful to keep two CD-ROM copies of all e-mail. For access control administration, an e-mail reply from an authorized person was taken as proof of authorization for access if only logged-in users could use the email system. 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 kept a record of incidents and their resolution, generating tickets to be sent to IT specialists when users reported a problem about the IT infrastructure.

Besides e-mail, a few participants used other tools like text or video chat to communicate. Again, perceptions of the usefulness of those tools 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.

Six participants (P1, P4, 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), and to show information to end-users about their IT security services (P10). In this last case, P10 employed an internal web site to show directly to users the status of their spam filters.

Interactions with different stakeholders made reporting an important feature of security tools. Our participants mentioned tools like Nessus (P9, P12, P21, P22), a tool used to scan vulnerabilities in the IT infrastructure; and McAffe ePolicy Orchestrator (P3, P4, P14), a tool used to summarize the virus activity of the systems. P9, who coordinated the mitigation of vulnerabilities with other IT specialists, 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. Our participants also mentioned other reporting features that security tools should include. P3 mentioned that security tools should generate reports that can demonstrate to stakeholders the economic benefits of applying security controls. Reports should also help security practitioners to prioritize their activities, showing the risks associated to the security vulnerabilities found (P4).

Complexity of Interactions

The eight activity types described by our participants show the diversity of IT security-related tasks and the importance of interactions in performing them. This diversity also speaks to the complexity of interactions with other stakeholders, which is expressed in the following aspects (see figure 2):

Multiple Stakeholders: Our participants had to communicate with other stakeholders that had *different perceptions of risks*, *considered security as second priority*, and *did not have security culture or training*. Our participants constantly had to persuade these stakeholders of the importance of security controls. In this process, participant's communication style was important in approaching stakeholders. Diplomacy was needed to achieve cooperation.

Multiple activities: Participants had to *exchange different types of information* and *spread security*

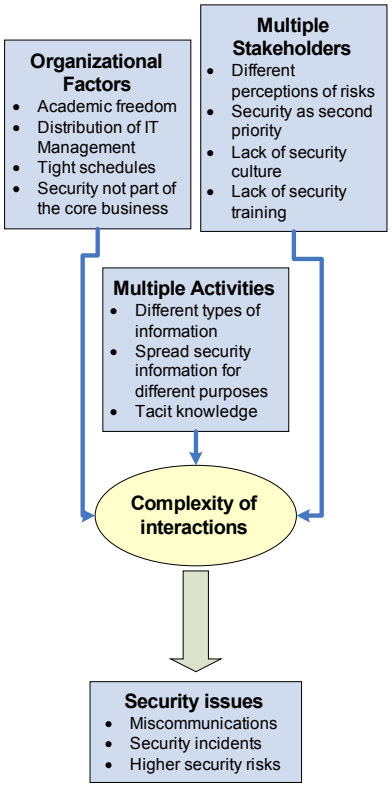

Figure 2: Model of the factors and consequences of complex interactions in the context of IT security.

information for different purposes to perform their activities. Examples of information exchanged were requirements (e.g., write a security policy), reports (e.g., vulnerability scans for audits), and notifications (e.g., alarms for security incidents). To spread this information, participants needed good communication skills to adapt interactions to the context of the activity. Participants had to use actively their *tacit knowledge* 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 with those tasks.

Consequences of complex interactions: We found that ineffective interactions can be the source of misunderstandings, security incidents, or can increase risk levels. For example, a lack of communication when making changes in firewalls can cause connection problems for other network users.

We are currently building a model that shows factors that determine the complexity of security interactions and the consequences of this complexity. This model will include organizational factors that exacerbate the complexity of interactions during security related activities (see figure 2).

Recommendations for Improving Tools

We next offer guidelines to improve security tools within this complex collaborative environment. Where possible, we indicate specific opportunities for those improvements:

Better support for collaboration: Goodall et al. [3] report on this need for one specific type of tool (intrusion detection systems), which should provide better support for security experts to collaborate with other experts around the world. Our empirical analysis extended this work by showing that security practitioners have to collaborate with a variety of stakeholders within an organization across many activities.

Decrease complexity: There are opportunities for tools to cut down the complexity of interactions that security practitioners have to face within organizations. Security practitioners need better reporting features to interpret the information from different communication channels. For example, 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.

Disseminate knowledge: Security practitioners need support for disseminating their knowledge within the organization. They have to be persuasive to communicate their knowledge about IT security and the importance of that security to other stakeholders, given the various priorities that different stakeholders may have. We identified the development of security policies as one way to communicate 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 organizational reality. However, the effectiveness of this dissemination process may be difficult to measure, as it is related to the security risks of the organization.

Provide flexible reporting: Previous analysis of a subset of the interviews [1] identified 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 the proposal by Chiasson et al. [2] to use *ecological interfaces* to design security systems, showing security information with different levels of detail depending on the user. Reporting in security systems also has to consider specific constraints, such

the employment of the need-to-know security principle. This constraint on communication is also mentioned by Haber and Kandogan, but as a characteristic of IT security administration [4]. Our analysis showed that this principle is used to both respect the confidentiality of information related to the investigation of violations of internal policies and to reduce the potential for miscommunication, by limiting communication to those stakeholders that lack enough background on security issues. Flexible reporting that incorporates specific security constraints is a field where developers can improve the communication features of security tools.

Integrate security tools and communication tools: 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 receive the information at the appropriate level of detail, language, and channel (e-mail, text message, web site).

Reduce communication overhead: Finally, tools could be more effective in showing relevant security configuration information to other stakeholders. For example, one of our participants used a feature of a spam filter tool to publish on a web page the status of users' e-mails. He thereby avoided questions from users about their e-mails when a new spam rule was added. We argue that this is yet another opportunity for improving communication support by security tools.

Conclusion

Our qualitative analysis reveals a complex environment where security practitioners not only perform security-specific tasks, but also interact with stakeholders with different backgrounds and needs. Security tools used by security practitioners do not provide enough support for this highly interactive environment. We have provided recommendations for integrating security tools for use with different communication channels.

These findings will provide the basis for further analysis of our data. We will continue the analysis of the remaining interviews, considering participants from a wider range of organizations. With this analysis, we plan not only to contrast and extend our results according to the type of organization and the position of the participant, but also to provide a testable model of the complexity of the interactions that can be used to guide improvement of security tools.

References

[1] D. Botta, R. Werlinger, A. Gagne, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding IT security professionals and their tools. In SOUPS, pages 100–111, July 2007.

[2] S. Chiasson, P. C. van Oorschot, and R. Biddle. Even experts deserve usable security: Design guidelines for security management systems. Presented at SOUPS USM, July 2007.

[3] J. R. Goodall, W. G. Lutters, and A. Komlodi. I know my network: Collaboration and expertise in intrusion detection. In CSCW, 63-90, November 2004.

[4] E. Haber and E. Kandogan. Security administrators: A breed apart. Presented at SOUPS USM, July 2007.

[5] E. Kandogan and E. M. Haber. Security administration tools and practices. In L. F. Cranor & S. Garfinkel, Editors, Security and Usability: Designing Secure Systems that People Can Use, 357–378. O'Reilly Sebastapol, 2005.

[6] 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.

[7] J. Redish. Expanding usability testing to evaluate complex systems. Journal of Usability Studies, 2(3): pages 102–111, 2007