Effectiveness of IT Security Tools in Practice

Fahimeh Raja[*], Kasia Muldner[†], Konstantin Beznosov[‡]

Laboratory for Education and Research in Secure Systems Engineering

lersse.ece.ubc.ca

University of British Columbia

Vancouver, Canada

Technical report LERSSE-TR-2008-XX[§]

Last Modification Date: 2008/04/28

Revision: #1

[*]fahimehr@ece.ubc.ca

[†]kmuldner@ece.ubc.ca

[‡]beznosov@ece.ubc.ca

[§]This and other LERSSE publications can be found at lersse-dl.ece.ubc.ca

Abstract

In today's world, IT security plays a critical role in different organizations, yet little is known about IT security in the context of organizations. This paper addresses this issue based on qualitative description analysis of 10 interviews with IT security practitioners from small to medium size organizations. Our results revealed the required knowledge and skills for effective IT security, IT security tasks, and the tools which are used to perform these tasks. Based on these results, we realized that current IT security tools can be improved in order to provide more effective support for security practitioners' activities. Founded on our analysis, we proposed some guidelines, such as regular update, settings for alerts, integrity of data, and effective logging of forensics information, in order to improve IT security tools.

Contents

1 Introduction

The increase in the application of information technology (IT) systems in different organizations as well as the increase in the number and type of threats to these systems makes IT security more critical than ever before. As reported by Sophos [sop], they discovered a new infected webpage every 5 seconds, in the first quarter of 2008. This is an average of more than 15,000 every day, three times more than in 2007.

IT security is also a costly element of organizations. The consequences of a single security breach could compromise the entire organization and cover a broad range of possibilities such as loss of time, money, and reputation. The results of a survey of 185 IT professionals from Network World Magazine's Technology Opinion Panel about the state of computer and data security in their organizations [sur] revealed that "more than 60% of IT managers felt that a data breach would cost their organization in excess of $10,000. Nearly 65% were very concerned that a data breach would result in public embarrassment and media scrutiny for their organization".

This shows the importance of effective IT security in organizations; however, to the best of our knowledge, little research has been done to study IT security practices in the context of organizations. According to [KC04], the reason may be the fact that developing a research in an organization-sensitive area requires major personal, financial and professional commitments far beyond what most researchers can afford to expend.

Our study is part of an ongoing field study, HOT Admin: Human, Organization, and Technology Centred Improvement of IT Security Administration. The main goal of this project is to investigate methods and techniques to improve IT security tasks and tools, considering the fact that human, organizational and technological factors affect the ability of IT security practitioners to do their job well.

In this paper, our aim is to study IT security in working environments in order to find how tools can affect the effectiveness of IT security practices in organizations. We use HOT Admin empirical data provided by semi-structured in-situ interviews with IT security practitioners from both academic and private sector. In the HOT Admin

project, several researchers are working on different pre-defined themes, such as IT security interactions, IT security challenges and IT security incidents [WHB08a, WHB08b]. This study continues the study by Botta et al. [BWG+07] on tasks and tools theme. We analyzed our data using qualitative description [San00] in order to gain insight in to details of IT security tools and practices. Our results support and extend the findings by Botta et al. [BWG+07] regarding the distributed nature of IT security in organizations, the skills and knowledge required for effective IT security, and necessary features for IT security tools. We also realized that current IT security tools can be improved in order to have more effective IT security in organizations. We proposed some guidelines that can be used in the development of IT security tools for more effective IT security.

1.1 Paper Organization

The rest of the paper is organized as follows. Section 2 discusses our related work. The methodology and execution steps of our study are described in section 3. Then, we discuss our results in section 4. Finally, section 5 concludes our paper.

2 Related Work

Botta et al. [BWG+07] reported their preliminary results of their field study of IT security tasks and tools based on the information gathered from 14 interviews with IT security practitioners. We have continued their study with more information from 10 more interviews.

Barret et al. [BHK+04] used grounded theory to study the typical tasks, tools, and environment of system administrators based on observations, diary entries, and survey data. Since system administrators may involve in IT security practices, their findings are relevant to our research; however, in our study we just focused on IT security practitioners who have special tasks, tools and behaviors [BHK+04].

Similar to our research, Kandogan and Harber [KH05] focused only on the area of security administration. In that study, they presented current practices of security

administration and discussed how tools support or fail them. Based on their findings from that research, they proposed some directions for improving the effectiveness of security administration tools. Unlike this study, in our study, we also consider how IT security responsibility is handled in organizations and what skills and knowledge are required for this purpose.

Bjrck [Bjö05] used grounded theory to study issues related to the management of information security in organizations. In this study a questionnaire with open ended questions and unstructured research interviews were used to collect the data. The motivation for this study is the need for cost efficient information security and the focus of the study is on organizational behavior that affects the management of information security. Unlike this study, we focused on how IT security practitioners perform their tasks and how they use their tools to carry out their tasks.

Anderson [And93] emphasizes on considering the environment in which security systems are to be used, especially system and human factors, in the development of security components. This study shows that "designers of cryptographic systems have suffered from a lack of information about how their products fail in practice". It shows that failures during installation and configuration of security systems were the most common sources of security problems in banks and governmental organizations. As such, we studied security practitioners in their real work place to see how they use their tools in practice and how these tools can be improved in order to make security practices more effective.

One of the areas in which HCI can be improved is security operation. There are several studies on usability of security applications [BDGS04, AS99, Kar89, WT99] which shows the impact of usability on effective IT security. We also consider usability of IT security tools on effective IT security.

Yee [Yee02] discusses that security and usability are not two opposite goals because both "want the computer to correctly do what the user want". This study looks forward to security systems that are more secure and usable not only in theory, but also in practice. In our research, we kept this in mind to study IT security practitioners' tasks and tools in their real work place to see how they use their tools in practice.

Zurko et al. [ZSS99] also places usability and security as peer goals in their design of an authorization service for distributed applications. This is an example of considering usability in designing security systems whose users are security practitioners (vs. end users). Similar to that study, the focus of our research is on IT security practitioners, not end users.

3 Methodology

In this study, qualitative methods have been applied to obtain and analyze data in order to answer the following research questions:

1. What tasks do IT security practitioners perform?
2. Which tools do they use?
3. How do they use these tools to perform their tasks?
4. Are their tools effective for maintaining IT security?
5. Which features of IT security tools can be improved for more effective IT security?

Our empirical data was collected from 10 audio-recorded semi-structured in-situ interviews with IT security practitioners from both academic and private sector. The type of these organizations and our participants' job description are shown in Table 1. In the interviews, our subjects were asked to answer several questions about different aspects of IT security in their particular organization, such as IT security activities and responsibilities, IT security tools, IT security skills, and communications. In order to decrease the interviewer's bias and to acquire details from different perspectives, each interview was conducted by two researchers. Each interview lasted about one hour.

We used qualitative description to analyze the interviews. We started with open coding and continued with axial coding [Cha06]. In the first step, open coding was used in order to conceptualize the data in the interviews. We coded all the instances of IT security tasks and tools in the interviews. We went back and forth while ana-

Table 1: Our participants' organizations and job description

Type of organization	Participant	Job description
Security consulting service	P23	IT security specialist
Non-profit medical service	P19	IT systems specialist
Manufacturing	P16	IT manager
	P21	IT security specialist
Academic 1	P17, P18	IT manager
	P20	IT system specialist
Academic 2	P22	IT system specialist

lyzing data. We constantly compared and modified the codes and eventually merged some of them into new codes. This phase yielded many codes; therefore, in the next step, we organized and classified these codes into higher level categories. Then, we reviewed and synthesized our results in order to get insight into them and obtain the big picture of the results to propose our guidelines and make the final conclusions. We evaluated our findings by comparing and contrasting them with the results of [BWG+07, WHB08b, KH05].

4 Results

Our analysis of the interviews gave us insight into how the responsibility of IT security is handled in organizations, what knowledge and skills SPs require to handle this responsibility, what tasks SPs carry out, which tools they use and how these tools can be improved for more effective IT security in organizations. In the following, we describe our results and a brief discussion for them.

4.1 IT Security in Organizations

In all of the organizations that we interviewed, the responsibility of IT security is shared among different people, usually affiliated with different organizational units

or groups: *"There is probably three people who spend the majority of their day having to do with security issues and one of them is in my group, which is in the networking area, so that's kind of the software parts of networking. One is in the systems group, and so then she is dealing with like system-type post type security type issues and the other person is also in the systems group but is taking care of more of the responsible use kinds of things"* (P15).

Although, several people deal with IT security in organizations, our interviews disclosed that IT security is not their main responsibility in their organizations. 8 of our participants were partially or indirectly responsible for IT security in their organizations: *"Well that's the appropriate title [Manager for the Network Management Center] for what I do because it involves kind of the whole realm of network services, where security is one piece of that. Security doesn't stand on its own because it's not just the network, it's also systems, it's also the host, and it's the applications as well"* (P15).

Discussion. Our results support the findings of [BWG+07] regarding the distribution of IT security responsibility in organizations and the fact that IT security is only one goal from different goals that SPs have.

Effective handling of distributed responsibility of IT security requires effective communication and collaboration between different individuals and groups. As it is discussed in [WHB08b, KH05], this communication and collaboration needs enough tool support to reduce the level of misunderstandings emerged in communications and the complexity of collaborated work.

4.2 IT Security Knowledge and Skills

Our interviews revealed that SPs apply different skills in their daily IT security practices. Beside the three necessary skills described in [BWG+07] - inferential analysis, pattern recognition, and bricolage - we found that communication skills are also essential for SPs. SPs require good communication skills for their interactions and collaborations with other SPs during their IT security activities. They also need this skill in order to convince others in their organization for having effective IT security.

They should know how to communicate IT security with top management that *"it is accepted as a business enabler rather than a roadblock"* (P25). They also should know how to interact with end users in order to handle user oriented problems and encourage the user to follow the IT security policies of their organization; for instance, P22 mentioned that s/he uses *"a friendly little e-mail chat"* with users when they violate IT security policies of their organization and P21 emphasized on *"a smile"* for handling this situation: *"Very nicely, with a smile on my face even though I'm talking on the phone because they can read that smile".*

Beside skills, the analysis of our interviews gave us insight into the knowledge required for effective IT security. SPs should have broad and deep technical knowledge in different areas of information technology: *"it is a work that requires you to have a wide range of knowledge about many different things. You have to be able to program an assembly if necessary. You have to understand UNIX systems, network systems, firewalls, Windows, everything. It's pretty much everything, software development, networking, operating systems work, pretty much everything - that's the beauty of it. You have to know a lot about a lot of things"* (P23). But, technical knowledge is not sufficient. According to four of our participants (P15, P22, P23, and P25), SPs require a holistic view of their organization as well: *"you really need to be able to look quite wide and deep. You need to be able to look within the packet in a lot of detail to understand how an intrusion detection system works, or a firewall is inspecting traffic. And at the same time you need to take a wide look to an organization to be able to determine okay where are the risks"* (P25).

Our interviews also disclosed that most of SPs' knowledge is in the form of tacit knowledge: *"A lot of them are not the kind of knowledge that can easily be codified"* (P23).

Discussion. Our results about skills support the findings by Botta et al. [BWG+07]. They highlighted inferential analysis, pattern recognition, and bricolage as the skills which are related to the use of tools; while we agree with that, we do not agree with their statement that communication skills *"have little impact with respect to tools"*. Because as it is discussed in [WHB08b], this communication is also related to the use

of tools. IT security tools can be improved in order to support SPs' communications more effectively. For example, communication features (such as text or voice chat) can be incorporated in to IT security tools for improving IT security effectiveness.

To support inferential analysis and pattern recognition skills, we recommend applying artificial intelligence, pattern matching, knowledge base and reasoning, and learning techniques in the development of IT security tools. To support bricolage, we recommend providing facilities for tools that supports combining several tools to perform a specific task: *"good support for adding packages and removing packages, usually binary packages that you fetch from somewhere"* (P20).

As mentioned before, SPs benefit from their tacit knowledge in performing their IT security tasks. This kind of knowledge is hard to access. However, the distributed nature of IT security and the diversity of knowledge required for effective IT security necessitate collaboration and knowledge sharing between SPs. To address this issue, we recommend documentation of complete process of IT security activities. It enables SPs to transform their tacit knowledge to explicit knowledge which is accessible by others. Documentation also has other benefits: *"That allows you to do two things: one is knowing what all the job functions people are carrying out and so if you have a concern about how something is being done you can tell its being handled by this individual team member versus that team member. It can also tell you areas where you can improve processes, where you have redundancies, where you can streamline and get efficiencies, and it can also tell you things that you've missed"* (P18). Therefore, IT security tools should provide facilities for documenting how SPs perform their tasks.

4.3 Tasks and Tools

Based on our interviews, we found that SPs are involved in miscellaneous tasks and they use different tools to perform these tasks. Table 3 shows the tasks that are performed by more than 50% of our participants (5 or more). It also shows the tools that our participants (at least one participant) use to carry out these tasks.

Discussion. There are tasks in Table 3 which may not be considered by tool devel-

opers. For example, one of the tasks of our participants which was not expected for us before this study is escalation. This task could be in several forms:

- SPs may escalate the problems with users to someone who has more executive power in organization: *"So this went back and forth a couple of times during the day and we ended up having to escalate that to our director because the person wasn't letting us either have access onto his system to be able to help him or to help do forensics or any kind of assistance. But he also wasn't letting us be able to have our network operate properly by being able to partition him off"* (P15)
- or they may escalate unusual requests to someone with more authority to decide about it: *"Occasionally they get specific requests and they know whether or not to escalate that to someone and say hey, this is outside of normal and they will escalate it"* (P16)
- or they may need to escalate security incidents to others in the organization: *"That person, she was actually very good about what she did and she escalated immediately to* 0142 *the university privacy officer, because it was a breach of privacy information"* (P17).

It shows that tool developers should consider the actual practices of SPs in their working environment to develop tools that effectively supports their different activities. For example, in the case of escalation, we recommend to provide facilities in IT security tools that support organizational flow of information.

4.3.1 Usability of IT Security Tools

The analysis of our interviews also revealed that all our participants agreed about usability of IT security tools: *"That's what makes a good tool to me. Ease of use, ease of use"* (P21).

One of our participants mentioned that s/he gave up using a newer version of a scanning tool (despite its better functionality compared to the older version) after a month because it was not easy to use for her/him: *"it was not intuitive, how it should be used"* (P23). This is interesting that this participant sacrifices more security for

Table 2: Our participants' common tasks and their tools

Task	Type of tool: Examples	Example of using a tool to perform the task	Description
Apply security patch	Tools for automatically apply security patch: Microsoft tool	To use Microsoft tool to apply patches to 50 workstations	To apply security patches to workstations and servers
Troubleshoot	Scripts	To use scripts to find failed logins and their IP addresses	To troubleshoot IT security problems by checking open ports, checking accounts, capturing packets, etc.
Prioritization	—	—	To prioritize activities, risk of vulnerabilities, or budget for purchasing security tools
Escalate	—	—	To escalate the problems with users to someone who has more executive power in organization; for example, when a user's computer is compromised, SPs may have to disconnect it from the network. If the user does not corporate with SPs in this case, they can escalate this problem to a manager.

Table 3: Our participants' common tasks and their tools (Continue of Table 2)

Task	Type of tool: Examples	Example of using a tool to perform the task	Description
Scan	Security scanner: nmap, Nessus	To run nmap to find open ports on the system	To scan system for running processes and open ports
Back up	—	—	Full and incremental back up of information
Training	—	—	To train other SPs, to train end users for policies and their commitments
Update	Email, Browser, Report: WSUS reports	To get email notifications for new patches	To be update with security news and alerts, software, tool and technology updates
Access control	Access control tools: Active Directory, SAP tool	To manage the permissions on files and print server in SAP	To manage users and their permissions for access to different resources in organizations such as physical equipments, operating systems, applications, databases, files, etc.
Monitor	System performance	Host monitoring tool: Nagios	To use monitoring scripts to find unusual high network traffic

more usability. This shows the importance of usability of IT security tools for more effective IT security.

The question that may arise here is what these participants mean by usability of tools. Our interviews show that these participants need IT security tools that are easy to install, set up, and run; that is, the order of actions to be followed should be determined and easy to remember. Their tools also should have understandable and intuitive user interface, i.e. interface with familiar features for them: *"If I can get information fast; fast and my uptime if fast If I have to struggle with it, it's not good for me you know like when you see buttons at the top, if they are buttons you are familiar with - like file save or file, you know what to do. If it says manage or whatever - whatever the buttons say at the top, if they are intuitive, you want it to just be intuitiveIf I have lots of time to play then it's okay. But I don't have lots of time to play. So I want to be able to get what I need and I want to get it now. And you want to be able to remember it"* (P21).

"For me, in terms of how my brain works, it works just fine in creating - I understand the user interface, if that makes sense" (P17).

"I would say Metasploit is quite challenging to install, the older versions of Nessus were - it just took a lot longer than it really should to install them and get up and running with them" (P25).

Discussion. Our results recommend considering usability and security as peer goals in developing IT security tools. This finding supports the results by [BWG+07, KH05, Yee02, ZSS99]. Beside understanding the necessity of these general usability guidelines [NM90] for IT security tools, by careful analyzing of how our participants use their tools to perform their tasks, we came up with several guidelines that could be considered in developing more effective IT security tools. In the following, we present each guideline with its related quotes from our participants.

4.3.2 Guidelines

- **Regular Update:** *"Today, it's changes on a rate of probably every three to six months. We are learning that what we did, literally, three to six months ago can no longer be done"* (P18).

  Because of ongoing changes in the world of IT security, we recommend that IT

security tools provide regular automatic update in order to prevent or detect and recover from new attacks and vulnerabilities: *"Nmap, Nessus, Webinspect, all these tools are updated quite regularly. If they didn't they would be useless for this kind of work"* (P23).

We also suggest that IT security tools provide SPs with the latest IT security news and alerts. As our interviews show, one of the common tasks between all our participants is to update. They read reports by special web sites on the Internet, such as Windows Server Update Service web site, or get email notifications for new vulnerabilities and new patches.

"Secunia is another one, I actually subscribe to backtrack and Secunia so as soon as vulnerability is posted to any of these lists I have a copy - I know on a day by day basis all the vulnerabilities that show up" (P22).

By adding the functionality of providing updates to IT security tools, SPs do not have to search for new IT security flaws and solutions, because tools take over this responsibility.

- **Settings for Getting Alerts:** As our interviews show, all our participants periodically examine their systems or check their reports and log files to find unintentional mistakes or unexpected and unusual activities.

  "We have Log Watch running and that reports nightly so the Log Watch is usually around a certain size and then I'll take a look at that in the mornings, so when we noticed, it was different" (P22).

  "You know periodically scanning our servers with nmap to make sure there are no suddenly open ports that I don't know about" (P20).

  Based on these findings, we recommend special settings in IT security tools which can be set by SPs in order to get alert under unusual or unexpected conditions; for example, in the case of P22, s/he can set these settings in order to get alert if the size of Log Watch report is greater than a threshold. In the case of P20, s/he can set the necessary open ports and get alert if there are other open ports than what s/he set before.

- **Less Overhead:** As Botta et al. [BWG+07] mentioned, IT security tools

should provide less overhead for SPs. Our interviews revealed that IT security tools should reduce overhead not only for SPs, but also for IT systems.

"Zero false negatives and zero false positives, that are really what you're aiming for Yeah but I mean if you can't achieve both then what would you prefer?... I would prefer less false negatives... If I had a choice, less false negatives and more false positives. Either way... more false positives means more work for you to do but at least you are being presented with a possibility that you can then eliminate. With a false negative you never get presented with the problem at all. So its there but you have no idea" (P23).

According to our participants (P20, P23, P25), IT security tools can reduce overhead for SPs by providing less false positives and less false negatives. P20 mentioned that s/he has to monitor IT systems and networks periodically in order to be alerted about suspicious behaviors; however, s/he sometimes neglect this duty because in her/his previous experiences of monitoring s/he *"got a lot of false positives and ended up being a lot of work for not very much benefit"*. This shows how the overhead originated from an IT security tool can result in less effective IT security.

Regarding the overhead for IT systems, P25 mentioned: *"I don't want something installing a lot of unnecessary software and making registry entries and just taking up more system resources"*. P19 also said that s/he switched from Symantec Anti-Virus corporate edition to Trend Micro Client Security because Symantec Anti-Virus corporate edition had a lot of overhead for their systems and did *"grind the systems to a halt"*. Therefore, we recommend considering less overhead both for SPs and IT systems in developing IT security tools.

- **Effective Logging of Forensics Information:** Our interviews disclosed that currently some IT security tools lack effective logging of information (P15, P17, P19, P21, P25). According to P17, they had to rebuild their whole IT system after an incident because they did not have enough logging information to analyze how their systems were compromised: *"That was where it necessitated rebuilding everything - because we couldn't get anything clear out of it. We hired*

an external forensics company to come in and they actually did a full analysis of all the servers that were affected and they were able to tell us the dates and times that they could locate from the forensics information on the first times the machines were hacked and then multiple times after that. They couldn't give us anything definitive as to how the data base in question was - how anybody got into it - because there just wasn't enough logging information for it" (P17).

Therefore, we recommend providing facilities in IT security tools for effective logging of forensics information in order to make the process of recovery from incidents more effective.

- **Integrity of Data:** According to P21 and P22, IT security tools should provide integrity of data in IT systems. P22 mentioned that in access control tools s/he requires facilities that *"blow out and affect the whole database"* when s/he makes some changes in users or their permissions. P21 also mentioned that they need to synchronize SAP and Active directory to provide consistency among their access control information. Based on these quotes, we recommend providing facilities in IT security tools for checking the integrity of data in IT systems.

- **Availability of IT Systems while doing Vulnerability Analysis:** *"anybody can throw a brick through a wall ... a glass pane in the shop front. It takes a bit more skill to actually break into the store and not trigger off any of the alarms"* (P23).

  Two of our participants (P21, P23) mentioned that the tools that they use for vulnerability analysis should not affect the availability of IT systems because it is important for organizations to have their system up and running.

  "But these are things you have to be careful with, that you don't inadvertently cause systems to shut down, or reboot or crash while you are doing this while at the same time still running a sufficient amount of tests that you are finding all the really important stuff and not missing things" (P23).

- **Provide both GUI and CLI:** Our interviews revealed that SPs use command line interfaces (CLI) or graphical user interfaces (GUI) based on their personal abilities and familiarity with these interfaces: *"I'm an old guy; I've been in the*

IT industry since before Windows. I grew up with DOS or even before DOS, with mainframes and stuff. So I am more familiar with the command line. I have better eye/hand coordination when I typing than when I'm moving the mouse around" (P23).

"I only use it for certain things. I don't know the Command Line. I don't know how to use them" (P21).

One of our participants also mentioned that s/he sometimes uses both of these interfaces to have different presentations of the same data (e.g., lists or graphs). Therefore, we suggest providing both GUI and CLI for IT security tools.

- **Flexible Reports:** In general, we found that our participants need *"clear and concise"* reports which enable them *"to get information that's meaningful without having to manipulate a lot of things"* (P21).

  Since IT security is distributed in organizations, IT security tools should provide appropriate reports for different people in organizations, e.g., reports for managers should provide them with an overview of security status of the organizations, while reports for SPs should provide technical details.

  "when I say info, I am a security person so I want info on users or roles or anything else to do with security. I don't want information on logistics" (P21).

  Moreover, IT security tools should provide reports in different formats (pdf, doc, spreadsheet, etc.) because different people in organizations prefer (and work with) different format of reports: *"So I could pull it all out and give them a spreadsheet and accountants love spreadsheets"* (P21).

  Since some organizations are periodically audited by external auditors for compliance with security regulations, we also recommend that IT security tools provide facilities to produce reports which are mandated by these auditors: *"It's got compliance managers, so in other words you can actually tell it, I want you to check for things that Sarbanes Oxley looks for. It says oh you want a test that Sarbanes Oxley is interested in and produces a report that is almost exactly what a Sarbanes Oxley auditor would be looking at"* (P21).

  One of our participants recommended to have the information from IT security

tools in a database *"so you can even run a third party reporting tool against it if you wanted to"* (P23). Although this helps flexible reporting, we recommend combining the third party reporting tool to IT security tools to facilitate the SPs' practices.

- **Flexibility:** SPs usually add their own functionalities or settings to their tools (P21, P22, P23): *"You see if a tool doesn't provide a particular solution in a particular way we just write our own"* (P22). Therefore, tools should be flexible so that SPs can customize them for their specific needs; for example, P21 likes Hyena (vs. Active directory) because it allows her/him to set the access permissions in a flexible way, at different levels of granularity: *"it lets me look at the file permissions down to - without having to look at each file separately, I can look at a whole container. I can look at the whole folder and all the permissions that are attached to every folder that's in there. So if I want to see a lot of information without having to go one at a time, every file, I use Hyena.*

- **Combine Data from Different Sources:** Our interviews show that SPs need to gather information from different sources and then combine, compare and analyze them: *"you have to gather information using many different tools and techniques and try and put together the information that does belong together to create a visual image of what it is you are trying to achieve"* (P22). *"Two different sources - well they are different sets of logs...Yes, so do you put them up on the same computer screen together in different windows or how exactly do you make the comparison?...Yes, you bring up all the logs on your screen so everybody has at least two screens that they use...You scroll up and down until you can see the things and compare them...Yes"* (P15).

  Therefore, IT security tools should provide facilities in order to not only provide information for SPs, but also combine different information from different sources, compare and analyze them. According to P23, currently IT security tools lack this feature: *"Nobody has actually bothered to put together an actual tool to provide a holistic solution...The tools are there, they do*

provide a lot of information but there is no tool that puts them all together".

Discussion. Based on the analysis of our interviews, we provide some guidelines to improve the effectiveness of IT security tools. Some of our guidelines, such as less overhead, provide both GUI and CLI, and flexible reporting are supported by findings of Botta et al. [BWG+07]. Flexible reporting is also supported by the results of [WHB08b, KH05]. What we recommend to develop for more effective IT security is a tool for managing information in IT security. A tool that updates information, gets information from different sources, combine and compare them, analyze them, provide flexible reports from them, prioritize SPs activities based on the information, and gives alerts in case of any suspicious behavior.

The strength of our study is that our results are based on the analysis of SPs activities in their real working environments. However, it has weaknesses too. One weakness of our study is that our results are only based on analyzing 10 interviews, what can be used to improve our methodology is participatory observation of how SPs use their tools in their practices.

5 Conclusions

This paper presents a qualitative analysis of IT security practitioners in their working environments. Our results validates the findings of Botta et.al [1] regarding the distributed nature of IT security and the skills required for effective IT security practices in organizations. We realized that current IT security tools are not effective to completely support different tasks and activities of SPs. Based on our analysis of how our participants use their tools to perform their tasks, we proposed some guidelines that can be considered in the development of IT security tools. We also provide literature [BWG+07, WHB08b, KH05] support for some of our guidelines from previous research. We believe that our results could be of interest to HCISec community.

References

[And93] Ross Anderson. Why cryptosystems fail. In *CCS '93: Proceedings of the 1st ACM conference on Computer and communications security*, pages 215–227. ACM Press, 1993.

[AS99] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[BDGS04] Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, and D.K. Smetters. In search of usable security: Five lessons from the field. *IEEE Security and Privacy*, 2(5):19–24, 2004.

[BHK+04] R. Barrett, E. Haber, E. Kandogan, P. Maglio, M. Prabaker, and L Takayama. Field Studies of Computer System Sdministrators: Analysis of System Management Tools and Practices. In *Proc. of the Conference on Computer Supported Collaborative Work*, pages 388–395, 2004.

[Bjö05] Fredrik J. Björck. *Discovering Information Security Management*. Doctoral thesis, Stockholm University, Royal Institute of Technology, 2005.

[BWG+07] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. Towards understanding IT security professionals and their tools. In *SOUPS*, pages 100–111, Pittsburgh, Pennsylvania, July 18-20 2007.

[Cha06] Kathy Charmaz. *Constructing Grounded Theory*. SAGE publications, 2006.

[Kar89] C.-M. Karat. Iterative usability testing of a security application. In *the Human Factors Society 33rd Annual Meeting*, 1989.

[KC04] Andrew G. Kotulic and Jan Guynes Clark. Why there aren't more information security research studies. *Information & Management*, 41(5):597–607, 2004.

[KH05] Eser Kandogan and Eben M. Haber. Security administration tools and practices. In Lorrie Faith Cranor and Simson Garfinkel, editors, *Se-*

curity and Usability: Designing Secure Systems that People Can Use, chapter 18, pages 357–378. O'Reilly Media, Inc., Sebastapol, 2005.

[NM90] Jakob Nielsen and Rolf Molich. Heuristic evaluation of user interfaces. In *CHI '90: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 249–256, New York, NY, USA, 1990. ACM.

[San00] Margarete Sandelowski. Whatever happened to qualitative description? *Research in Nursing & Health*, 23(4):334–340, 2000.

[sop] http://www.sophos.com/pressoffice/news/articles/2008/04/secrep08q1.html.

[sur] http://www.findwhitepapers.com/resource/vid2/whitepaper2256/index.php.

[WHB08a] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. In *to appear in HAISA'08: Human Aspects of Information Security and Assurance (10 pages)*, July 2008.

[WHB08b] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. Security practitioners in context: Their activities and interactions. In *Presented at Student Research Competition Poster Session, ACM SIG CHI Conference*, page 6 pages, 2008.

[WT99] Alma Whitten and J.D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium*, pages 169–184, 1999.

[Yee02] Ka-Ping Yee. User interaction design for secure systems. In *ICICS '02: Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290, London, UK, 2002. Springer-Verlag.

[ZSS99] M.E. Zurko, R. Simon, and T Sanfilippo. A user-centered, modular authorization service built on an RBAC foundation. In *IEEE Symposium on Security and Privacy*, pages 57–71, Oakland, CA , USA, 1999.