Identifying Differences Between Security and Other IT Professionals: a Qualitative Analysis

A. Gagné, K. Muldner and K. Beznosov

Laboratory for Education and Research in Secure Systems Engineering
University of British Columbia
Vancouver, Canada
e-mail:{andreg, kmuldner, beznosov}@ece.ubc.ca

Abstract

We report factors differentiating security and other IT responsibilities. Our findings are based on a qualitative analysis of data from 27 interviews across 11 distinct organizations. The results show that compared to other IT, security professionals have to manage a higher level of complexity, stemming from factors such as the need to balance usability and security, negative stakeholder perception, and external threats. We synthesize the differences into an overall model and discuss how the model can guide the development of support for professionals with security responsibilities.

Keywords

Security Administration, Qualitative Analysis, Information Security Culture

1. Introduction

Given that information technology (IT) has become pervasive in today's organizations, properly securing systems is critical. However, many challenges remain with respect to implementing sound technologies and security processes. In the past decade, the research focus has shifted, from only exploring technological solutions to also include organizational and human factors, as these factors play a key role in influencing security practices and outcomes (e.g., Kraemer and Carayon, 2007). To date, however, little work has targeted the population that is at the crossroads of these factors, namely security professionals, who are responsible for protecting their organizations from IT-related threats. Currently, these individuals lack sufficient organizational and technical support, as is evident by the rising number and cost of security incidents (Bagchi and Udo, 2003). As a first step in gaining insight on how to provide this support, we evaluated how security differs from other IT activities, in terms of skills required, environment, etc. We chose to focus on this avenue for two reasons. First, an understanding of the differences will shed light on security professionals' needs, thereby providing direction for future research on devising effective solutions. Second, security is a less mature field than IT in general, and as such, could borrow insights from IT, but only if a clear understanding exists on how the two fields relate.

To obtain a rich perspective on the why and how of factors relating security and other IT, we employed a qualitative approach of *in situ* interviews with professionals from a variety of organizations. Our research was part of a larger project with the overall goal of supporting security professionals through innovative technological solutions that take into account the human, organizational and technological factors influencing security professionals (Botta et al., 2007). In this paper, we provide an in-depth analysis of data gathered from 27 interviews that highlights a number of key differences between security and other IT. In doing so, our research brings the following contributions: (1) we validate existing work on isolating differences between security and other IT with a larger and more diverse set of data; (2) we extend existing work by (i) isolating key differences related to human and organizational factors, such as the usability vs. security trade-off, a factor that plays a vital role in influencing security professionals and stakeholders' perceptions of them; (ii) providing a model relating the various differences.

In the following discussion, we rely on the approach in Haber and Kandogan (2007) and distinguish between IT professionals who have security responsibilities (security professional, *SP* from now on) and other professionals who are responsible for IT work without a security element (general IT professional, *genIT* from now on). We begin by presenting related work. We then describe our methodology in Section 3. Section 4 presents our findings, which we discuss in Section 5.

2. Related Work

The related work can be classified among two dimensions: (1) research that focuses on system administrators (sysAdmins), without distinguishing between security and other IT work or identifying if a professional even has security duties, and (2) research that focuses on security professionals (SPs).

Haber and Bailey (2007) relies on naturalistic observation to study sysAdmins in six organizations. Their major findings are that sysAdmins need better tool support and that compared to end-users, sysAdmins deal with larger, more complex systems and face a higher risk of failure. Barrett et al. (2004) conducts 12 interviews with sysAdmins and their managers at six organizations. The results highlight the collaborative nature of sysAdmin's work, as well as that sysAdmins rely heavily on technical, social, and organizational skills in a highly complex environment. Anderson (2002) conducts a survey of related work and participants from USENIX Large Installation System Administration (LISA). The analysis reveals that the sysAdmins' primary tasks includes maintenance, reconfiguration, and end-user training, and that dependability and automation of these tasks is at the forefront of sysAdmins' concerns. Halprin (1998) provides guidelines for sysAdmins; major recommendations include reducing sysAdmins' distractions and automating tasks to reduce the burden on sysAdmins.

Other work focuses on security professionals. Siegel et al. (2006) perform contextual inquiry of 30 SPs at three organizations. The findings show that IT security is distributed as a secondary task or goal, and that there is a lack of documentation and

automation. In addition, the findings also suggest that a lack of management buy-in influences SPs' ability to be proactive, and that SPs have difficulty effectively communicating with organizational stakeholders, which reduces management buy-in. Haber and Kandogan (2007) focus on identifying differences between security and other IT professionals. To identify differences, they rely on a subset of interviews conducted for Haber and Bailey (2007), namely four interviews from one academic organization. The findings show that SPs have to contend with a higher level of complexity, stemming from the need for a wider overview of the organization, a higher level of risk, the need to be more proactive and collaborate more with other stakeholders.

3. Methodology

To obtain realistic data grounded in actual experiences, we conducted 27 *in situ* semi-structured interviews over a period of 15 months. The corresponding 27 participants (P1-P27) worked for a wide variety of organizations (11 different organizations in total, from 7 sectors, see Table 1). The participants' positions ranged from IT manager to specialized security professional (see Table 1). All participants devoted some time specifically to security; most also performed other non-security IT tasks (and all have been responsible for non-security IT duties at some point in their careers). As all of our participants had experience with both security and other IT work, this placed them in a unique position to contrast their security responsibilities with other IT tasks. We should point out that some IT professionals do focus solely on IT tasks that do not have a security element, as our participants mentioned, and as was found in other research (e.g., Haber and Kandogan, 2007).

Position	Description	Participant ID_{ORG*}
IT: Manager	Manages all aspects of IT, including security	$P1_{Edu}$, $P15_{Edu}$, $P16_{Man}$, $P18_{Edu}$, $P23_{Con}$
IT: General	Performs a diverse range of IT-related duties, including security	$P10_{Edu}$, $P12_{Sci}$, $P19_{Non}$, $P20_{Edu}$, $P26_{Con}$
IT: Specialized	Works in a specific area of IT and is responsible for security in that area	$P6_{Edu}$, $P7_{Edu}$, $P8_{Edu}$, $P13_{Sci}$, $P14_{Edu}$, $P22_{Edu}$
Security: Manager	Manages security, including staff, design of policy, etc.	$P2_{Edu}$, $P27_{Con}$
Security: General	Performs a diverse range of security-related duties	$P5_{Ins}$, $P17_{Edu}$
Security: Specialized	Works in a specific area of security	$P3_{Edu}$, $P4_{Fin}$, $P9_{Edu}$, $P11_{Edu}$, $P21_{Man}$, $P24_{Edu}$, $P25_{Fin}$

*The subscripts correspond to organizational sector: Post-Secondary Educational (Edu), Financial Services (Fin), Insurance (Ins), Scientific Services (Sci), Manufacturing (Man), Non-profit (Non), Consulting (Con).

Table 1: Participant Information

During the *in* sit*u* interview, participants were asked a variety of security-related questions (e.g., challenges, tools, organizational influences, security vs. other IT). Each interview lasted approximately one hour. The interviews were transcribed, sanitized to preserve the participants' anonymity, and subsequently analyzed. For the analysis, our primary research question was: *What differentiates security from other IT work*? To answer this question, we relied on qualitative description (Sandelowski, 2000). This involved: (1) identifying in each transcript instances that contained information related to our research question; (2) iterative coding, that began with open coding (i.e., selection of categories that arise from the analysis of the data) and moved to axial coding (i.e., synthesis and refinement of the data, to make explicit the connections between the categories).

4. Results

Our analysis revealed the following themes characterizing the key differences between security and other IT: *security vs. usability, stakeholder perception, complexity of troubleshooting, environment* and *maintaining scope*. It is important to note that (1) these themes are based on our participants' data, and not intended to necessarily provide a comprehensive survey of all the differences; (2) as is typically the case with semi-structured interviews, not all participants were asked the same questions, and not all discussed differences between security and other IT.

4.1. Security vs. Usability

A key factor differentiating security from other IT is that the former requires SPs to constantly balance the trade-off between making technology secure and usable. As one participant expressed it, "*I think it [security] is different because you have to balance the usability of the system you are creating security for as well as the security. You can have a foolproof security system but it's not going to be very usable... the most secure system is when it's turned off, and behind locked doors*" (P19). In contrast, genIT professionals are predominantly concerned with making technology work, and so do not have to consider this trade-off (P18). P19 echoed this sentiment, stating that "*If I was just building desktops for people and security wasn't a concern, it's easy*".

For SPs, finding the right balance in making the trade-off is particularly challenging, since increased security is often a hindrance to performance (P20, P4). Consequently, SPs aim to be as strict as possible, while still allowing users to do their work (P19). An example mentioned by one participant related to access (P23). Specifically, one organization had the practice of hiring temporary workers, and had to provide them with access to data, while at the same time balancing privacy considerations. The security/usability trade-off did mean that security sometimes impeded function (P3). One participant went as far as saying that security is different from other IT because "*security involves making things more difficult for people*" (P20).

4.2. Stakeholder Perception

Our data shows that genIT professionals tend to be perceived in a more positive light than SPs. According to one participant, this perception stems from the nature of security, since "*all other IT activities are perceived more as enabling the business to do their work, where security is the one group that is perceived as the opposite*" (P25). This observation that in contrast to other IT, stakeholders perceive security measures as a hindrance to operations was echoed by other participants (P3, P16, P13). SPs are seen as enforcers: *"[there is this perception] that we were standing with a big stick waiting to hit them, in case they did something wrong*" (P1). This "*us vs. them*" perception may make it difficult for SPs to persuade stakeholders of the need to implement sound security measures. Effective persuasion is key, given that security is typically not a primary concern for stakeholders, who prefer to focus on tasks that keep the business running (P17). Typically, the only time security is a focus is "*when something bad happens*" (P1, P23, P24).

To influence stakeholders' perception and convince them to engage in best practices, SPs need to promote security and educate (P23, P19, P14). As one participant expressed it, "*I gotta make them a) understand the situation, b) get excited and motivated to actually wanna do something about it*" (P3). Another strategy our participants employed involved promoting awareness of legislation: "*we want people to be aware of privacy and privacy legislation and what their commitments are*" (P23). Yet another tactic for convincing stakeholders involved being open and accessible and "*really having that collegial relationship*" (P2).

4.3. Complexity of Troubleshooting

Both SPs and genITs have to contend with high complexity in their daily activities, however, our participants felt that compared with other IT, security tasks entail a higher degree of complexity. An activity that participants chose to focus on to highlight this difference was troubleshooting. SPs and genITs professionals are both required to perform troubleshooting, for instance, to diagnose why a network server is not functioning properly, and/or to determine if a security breach has occurred. However, our participants pointed out that when dealing with security issues, troubleshooting is more complex, because "*you usually have to go through a lot more steps to try and figure out where the problem is occurring" (P15).* This participant goes on to say that troubleshooting is less complex for other IT work, because in security, you *"have to work with somebody else*". P26 also chose to focus on troubleshooting as the key difference between security and other IT work, pointing out that troubleshooting security-related problems required a wide variety of tools, verification and testing.

Our participants mentioned several other factors that they felt increased troubleshooting complexity of security tasks, including (1) uncertainty, (2) reliance on tacit knowledge, i.e., knowledge that can only be gained via experience, and (3) sensitive nature of the process (note that the first two factors are likely not specific to security). The analysis process for security tasks is permeated with uncertainty,

making it difficult to determine that it was done correctly. P4 described one such instance: "*I was able to track down the service provider and I was actually able to bring down that [offending] site but still, in the back of my mind it was too easy… just too many weird things about it*". Also complicating troubleshooting is that it requires tacit knowledge, which can only be gained through experience, for instance to diagnose whether error messages actually signal a security issue (P9). Finally, compared to genIT professionals, SPs have to contend with more sensitive "*human*" issues with greater consequences, which influence the troubleshooting process and its impact. As far as the process is concerned, security tasks may require that SPs are given access to stakeholders' personal computers, which can involve "*potential privacy issues*" (P20). With respect to the impact of troubleshooting, the cost of reporting security incidents can be very high: "*you cannot jump to conclusions and assume someone is guilty - more is at stake than simply how fast the system is recovered* " (P5).

4.4. Environment

The IT infrastructure in the workplace is continually growing more complex, with the advent of wireless networks, cell phones, PDA's and other devices. For security tasks, this changing technological landscape has influenced security practices, calling for a defense in depth strategy. Furthermore, not only is the technological landscape constantly changing, but it is doing so quickly. One participant chose to focus on this dimension, i.e., rate of change, when discussing the difference between security and other IT, by pointing out that "*IT is a fast changing field and security is even faster* " (P2). A likely cause of this difference relates to threats.

GenIT professionals certainly have threats to contend with, such as for instance power outages that take down servers and impact organizational productivity. However, only SPs have to contend with active and continuous threats, i.e., agents that deliberately aim to compromise the organization. These threats take on a variety of forms and influence both the SPs who have to deal with them and the organization as a whole. One participant mentioned the impact of hardware theft, saying that "*It was very, very expensive to fix [and resulted in many] man hours lost and stakeholder time*" (P6). Illegal access to information was a threat mentioned by another participant, claiming it to be "*the biggest risk* " (P5). P20 also mentioned illegal access to data as the primary threat, as it involved privacy implications. These threat agents can have devastating consequences. A key concern for our participants was liability (P1, P19), since compromise of personal data could lead to lawsuits and even prison time for the organizational executives (P19). Another concern for our participants was loss of service. P14 mentioned that a security incident resulted in the loss of several servers; P25 stressed that denial of service attacks were the key concern, since loss of service had an "*extremely high cost*".

Our participants mentioned two direct consequences of having to contend with a fast-paced environment that involves active threats: (1) *need for fast response time* and (2) *need to be up to date*. Given the fast-paced IT environment, both security and other IT tasks require a timely response. However, the nature of security means that a

speedy response is particularly critical, for a number of reasons. First, security problems can involve privacy breaches that expose sensitive data, where the degree of exposure may depend on the ability of professionals to immediately address the breach. Second, reacting quickly to catch individuals compromising security in an organization may cause a shift in organizational culture to prevent such behaviour in the future (P5). To manage the need for a fast response time, SPs have to be proactive; one participant mentioned that firewall logs are reviewed on a daily basis so that security breaches can be addressed immediately (P4). Furthermore, SPs have to constantly keep up to date via education, in order to keep abreast of new risks and policies (P18, P4, P2, P6). This education is a daily ritual for SPs: "*in the morning I usually try to get up early and check what is going on in the IT security world* " (P4). To keep up to date, our participants also read publications (P6) and news groups to identify new vulnerabilities (P2).

4.5. Maintaining Scope

Several of our participants chose to focus on scope as a key difference between security and other IT (P19, P25). One participant pointed out that only security requires maintaining a wide and deep overview of the organization, "*I would say that probably nobody else really looks at the organization in the same way as security members, 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. And at the same time you need to take a wide look to an organization to be able to determine the risks. And that differs from IT where other groups can really be focused in one particular area*" (P25). The need for a wide overview is a consequence of the distributed nature of security. For many of our participants, the responsibility of upholding security was distributed (P1, P2, P4, P11, P14), since as P1 stated, "*one person can't do everything*". This distribution increased the complexity of daily tasks, as it required various stakeholders to troubleshoot and resolve issues (P11, P14); here, a lack of cooperation was a challenge: "*it becomes very difficult, the level of cooperation. I can't get the three Novell administrators to even send me an acknowledgement of an e-mail about something that affects them - it's very frustrating and it delayed our deployment*" (P1).

In addition to the need for a broad *internal* scope, factors unique to security require SPs to maintain a broad *external* scope. One of these factors, a complex environment driving the need to be proactive and up to date, was described in Section 4.4. Another factor is the need for SPs to account for legislation. P7 described how the Patriot Act, which aims to ensure data privacy, hinders some security tasks because it is so strict. Legislation impacts not only data access, but also archiving practices. P21 described how project approvals are archived in case an audit occurs, to verify compliance with the Sarbanes-Oxley Act (SOX). Another participant described archiving email communications for tasks that "*might go legal* ", in order to have a paper trail (P1).

5. Discussion

Our analysis uncovered a number of key differences between security and other IT, and in doing so, validated and extended existing research. We validated research that explores differences between security and other IT, by confirming Haber and Kandogan (2007)'s findings related to complexity, a fast-paced environment, and the need to be proactive and up to date. We extended their work as follows. First, we exposed differences related to human and organizational factors, namely the usability/security trade-off, stakeholder perception of SPs and the need for SPs to promote security. While Siegel et al. (2006) also found that stakeholders' negative perception is a challenge for SPs, we showed this to be a unique difference between security and other IT. Second, we provided a rich description of the differences by involving a larger and more diverse set of participants. In particular, whereas Haber and Kandogan (2007) relied on data related to SPs from one academic organization, we substantially increased the scope by including 27 participants from 11 different organizations. Third, we developed a model that provides an overall view of the various differences and the interconnections between them, shown in Figure 1, which we describe shortly.

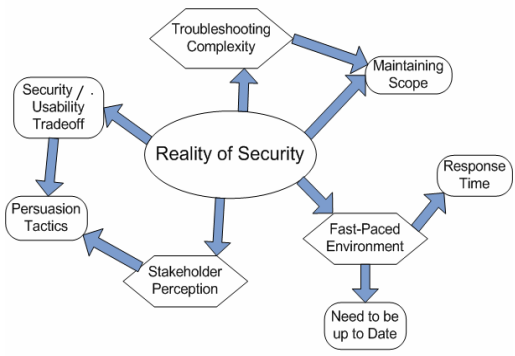

Figure 1: Differences between security and other IT as highlighted by our analysis; arrows are directed from causes to outcomes. Differences pertaining to factors influencing SPs are shown as hexagons; differences pertaining to SPs' behaviors are shown as rounded rectangles.

In general, the differences between security and other IT activities increase the overall complexity SPs have to contend with. In particular, SPs have to balance security with usability in a fast-paced and complex environment, try to mitigate negative stakeholder perception, while maintaining a deep and broad overview of the organization, to name a few. We propose that future research directions should aim to reduce this complexity associated with security work. To aid such endeavors, we synthesized the differences revealed through our analysis into an overall model (Figure 1). In the model, the arrows are directed from causes to outcomes, where some of the differences are a direct consequence of the reality of today's security technologies (see *Reality of Security*); these differences are in turn the driving force

for other differences. For instance, existing technologies do not seamlessly integrate security tasks with users' primary tasks, requiring SPs to make the usability/security trade-off. This in turn requires SPs to employ persuasion tactics to motivate stakeholders to engage in effective security practices. In addition to synthesizing the differences, we also categorized the various differences, as either:

- factors that impact SPs (shown as hexagons in Figure 1, and include *Troubleshooting Complexity, Fast-paced Environment* and *Stakeholder Perception*), or
- SPs' behaviors as a response of the above factors and/or the reality of security (shown as rounded rectangles in Figure 1, and include *Maintaining Scope, Response Time, Need to be up to Date*, *Security/Usability Trade-off* and *Persuasion Tactics*).

The distinction between the two classes of differences, factors influencing SPs vs. SPs' direct behaviors, shows how factors and/or the reality of security influence SPs' actions. In doing so, this distinction highlights the root cause for SPs' behaviors, allowing research endeavors to target solutions to decrease the complexity not only at the source but also at its origin. In general, the model allows researchers to understand not only the root cause of a difference, but also how a particular solution aiming to reduce complexity related to that difference may impact other facets of SPs' activities. For instance, a solution that reduces the need for SPs to make the usability/security trade-off in turn should reduce the need for SPs to engage in persuasion tactics. We now discuss several specific suggestions with respect to lowering the burden on SPs arising from the complexity highlighted by the differences between security and other IT. These suggestions encompass both technological and organizational aspects, as the practice of security is inherently a multi-faceted activity requiring an interdisciplinary approach.

Troubleshooting Complexity. The distributed nature of security drives the need for SPs to interact with various stakeholders during troubleshooting, thereby increasing its complexity. Our impression based on the interviews is that currently very little support exists for scaffolding interactions between SPs and other stakeholders. Thus, solutions that support interaction within the activity of troubleshooting could reduce some of the related complexity. Troubleshooting is also made challenging by the need to employ tacit knowledge, another consequence of the reality of security. We propose that business process management tools may help to document, update, and retrieve information corresponding to SPs' tacit knowledge. As one of our participants stressed, the success of such systems is strongly dependent on appropriate tactics organizations employ to encourage their use. This participant successfully utilized the rule that an individual "owns" a particular solution or process and is solely responsible for that process until he or she documents it.

Stakeholder Perception. We propose that one way to mitigate stakeholders' negative perception of SP is via management who is committed to having a secure organization, a suggestion echoed in Siegel et al. (2006). CEO's can set organizational culture and managers can lobby for change. Effective proactive educational tactics can have a profound effect on security culture. For instance, in

contrast to the majority of the participants we interviewed, P27 felt that lack of stakeholder buy-in with respect to effective security practices was not an issue, largely due to the success of innovative educational campaigns that were a routine event at this participant's organization.

Security vs. Usability. Our analysis highlighted that SPs are constantly aiming to balance security with usability. We propose that some of this burden can be alleviated through a shift in design culture, i.e., via alternative ways of building security technologies that reflect user needs. For instance, security tasks could be seamlessly integrated into daily IT activities, rather than treated as separate tasks requiring explicit user attention (as proposed in Smetters and Grinter, 2002). Now, this may not always be possible, however, our findings and other research (e.g., Smetters and Grinter, 2002) suggest that today there are insufficient attempts in this direction. Another option to increase the usability of security technologies is to involve stakeholders during the design process (as in Flechais and Sasse, in press), which helps to identify their needs and increases the chances of reaching a usable solution.

6. Conclusions and Future Work

Although SPs bear the burden of securing organizations, we have yet to reach an understanding on how to best support them in their daily tasks. To further this understanding, we analyzed the relation between security and other IT. Our analysis revealed a number of differences, stemming from factors such as the need to balance usability and security, negative stakeholder perception, and external threats. The differences increase the complexity of SPs' processes and practices, highlighting the need for innovative solutions to support this population. To aid this process, we provide a model that characterizes the interconnections between the various differences, and so enables researchers to understand how a corresponding solution may influence other aspects of SPs' work. As the next steps, we plan to (1) refine this model with additional data and analysis, and (2) rely on the model, as well as related work, to identify if and how support designed for genIT professionals may be transferred over to aid SPs. As far as the first step is concerned, we are especially interested in two directions. First, we intend to collect data from other organizational sectors, and analyze how our findings generalize to other types of organizations. Second, we plan to examine how factors such as organizational size and position (e.g., manager, specialist) influence the differences between security and other IT.

References

Anderson, J. (2002). Researching System Administration. PhD thesis, University of California.

Bagchi, K., Udo, G. (2003). An analysis of the growth of computer and internet security breaches. Communications of the AIS, 12(46), p. 684–700.

Barrett, R., Haber, E., Kandogan, E., Maglio, P., Prabaker, M. and Takayama, L. (2004). Field Studies of Computer System Administrators: Analysis of System Management Tools and

Practices. In Proc. of the Conference on Computer Supported Collaborative Work, p. 388–395.

Botta, D., Werlinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. (2007). Towards understanding IT security professionals and their tools. In SOUPS, 1p. 00–111.

Flechais, I. and Sasse, M. (2008). Stakeholder involvement, motivation, responsibility, communication: how to design usable security in e-science. Int. Journal of Human-Computer Studies, in press.

Haber, E. and Kandogan, E. (2007). Security administrators: A breed apart. In Proc. of SOUPS Workshop on Usable IT Security Management (USM), 4 pages.

Haber, E. and Bailey, J. (2007). Design Guidelines for System Administration: Tools Developed through Ethnographic Field Studies. In Proc. of 2007 symposium on Computer human interaction for the management of information technology (CHIMIT), 9 pages.

Halprin, G. (1998). The Work Flow of System Administration. In Proceedings of the 6th Annual Conference of the System Administrators Guild of Australia SAGE − AU '98.

Kraemer, S. and Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38, 14, p. 3–154.

Sandelowski, M. (2000) Whatever happened to qualitative description? Research in Nursing & Health, 23(4), 3, p.34–340.

Siegel, D., Reid, B. and Dray, S. (2006) IT Security: Protecting Organizations In Spite of Themselves. Interactions, p. 20–27.

Smetters, D. and Grinter, R. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In Proc. of the Workshop on New Security Paradigms, p. 82–89.