Human, Organizational, and Technological Factors of IT Security

Kirstie Hawkey
University of British Columbia
4044-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
hawkey@ece.ubc.ca

Andre Gagne
University of British Columbia
4085-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
andreg@ece.ubc.ca

David Botta
University of British Columbia
4085-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
botta@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
4047-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
beznosov@ece.ubc.ca

Rodrigo Werlinger
University of British Columbia
4085-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
rodrigow@ece.ubc.ca

Kasia Muldner
University of British Columbia
4044-2332 Main Mall
Vancouver, BC V6T 1Z4 CAN
muldner@ece.ubc.ca

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

Abstract
This paper describes the HOT Admin research project, which is investigating the human, organizational, and technological factors of IT security from the perspective of security practitioners. We use qualitative methods to examine their experiences along several themes including: unique characteristics of this population, the challenges they face within the organization, their activities, their collaborative interactions with other stakeholders, the sub-optimal situations they face as a result of distributed security management, and the impact of the security management model in place. We present preliminary results for each theme, as well as the implications of these results on the field of usable security and other research areas within HCI.

Keywords
IT Security, human factors, organizational factors, technological factors, qualitative research

ACM Classification Keywords
H5.3. Information interfaces and presentation: Group and Organization Interfaces – *Collaborative Computing*.
K6.5. Management of Computing and Information Systems: Security and Protection

The HOT Admin Project
Information security has become a critical issue for organizations as they must protect their information

figure 1: The work of security practitioners work is impacted by human, organizational, and technological factors.

assets from unauthorized access and quickly resume business activities after a security breach. It is necessary to broaden the study of security issues to include not only the technical, but also the human and organizational dimensions [11]. A better understanding of real world conditions and constraints during the adoption of security practices would help developers and designers make secure systems more usable [3].

To date, there is little empirical evidence about how human, organizational, and technological factors impact IT security management (ITSM) [5, 10]. Moreover, little is known about the responsibilities and roles of security practitioners (SPs) or the effectiveness of their tools and ITSM practices [5]. The Human, Organization, and Technology Centred Improvement of IT Security Administration (HOT Admin) research project is working to fill that gap (figure 1).

The main goals of the HOT Admin project are: 1) to devise a methodology for evaluating the usability of IT security tools; and 2) to design effective technological solutions and guidelines to aid SPs. The first phase is a field study that aims to build a holistic view of how SPs practice ITSM within the realities of their workplaces.

The research we are conducting is timely and complements other preliminary work in this emerging field. We next describe the field study methodology and our participants. We then summarize six independent research thrusts and our findings to date. These include: 1) the unique needs of IT SPs, 2) the challenges they face when implementing IT security in organizations, 3) the impact of security management models, 4) their responsibilities and tasks, including security incident response, 5) their collaborative interactions with other stakeholders within the organization, and 6) the sub-optimal situations they face as a result of distributed IT security management.

Methodology

Data collection consists of questionnaires, semi-structured in-situ interviews, and participatory observation. To reduce bias, two researchers conducted each interview. The interviews were analyzed along each research theme, using qualitative description with constant comparison and inductive analysis of the data. The interview questions were periodically revised to validate emerging theories. For the overall project, five researchers performed the analysis, each focusing on different themes. Overlap of concepts between themes allowed triangulation of analysis at the researcher level.

Participants

To date, we have conducted 34 semi-structured interviews with a total of 35 participants from 16 unique organizations (table 1). The breadth in organization types and security positions has allowed us to validate and generalize prior findings from studies with a narrower focus as well as contribute new knowledge to this emerging field.

Results to Date

Preliminary general results from the first 14 participants were presented at SOUPS [1]. These results highlighted the distributed nature of IT security management across the organization and gave an initial sense of the skills necessary for practitioners. This preliminary analysis helped shaped the research themes currently under analysis and/or submission. We now give a brief introduction to each theme as well as a sense of the results that have emerged to date.

Number and position of participants for each Organization Type
Academic (3)
4 IT Managers
1 Security Manager
4 Security Specialists
9 IT (with security tasks)
Financial Services (2)
2 Security Specialists
Insurance (1)
2 Security Specialists
Scientific Services (1)
2 IT (with security tasks)
Manufacturing (1)
1 IT Manager
1 Security Specialist
Retail/Wholesale Sales (1)
1 Security Specialist
Governmental Agency (1)
1 Security Manager
Telecommunications (1)
1 Security Manager
Non-Profit Organization (1)
1 IT (with security tasks)
Technology (1)
2 Security Managers
IT Consulting Firm (3)
1 Security Specialist
2 IT (with security tasks)

table 1: For each organization type, we indicate the number of unique organizations and give the number of IT Managers, IT Practitioners (with security tasks), Security Managers, and Security Specialists interviewed.

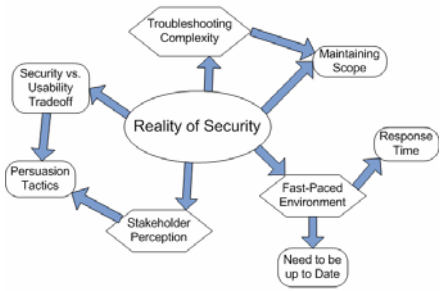

figure 2: Aspects of information security management that distinguish security practitioners from general IT professionals.

Unique Characteristics of Security Practitioners

We are evaluating how security and general IT staff differ in terms of behaviours, skills, and environment. An understanding of these differences will shed light on security professionals' needs, thereby providing direction for future research. Furthermore, insights could be borrowed from general IT, but only if we have a clear understanding of how the two fields relate.

Our findings validate and generalize prior work [4], by confirming differences related to complexity, a fast-paced environment, and the need to be proactive and up to date (figure 2). We found new differences related to human and organizational factors, such as a usability vs. security trade-off, a perception of SPs by other stakeholders, and a need for SPs to promote security.

Security Management Challenges

While some studies have investigated a subset of ITSM challenges (e.g., [6, 9]), none have provided a comprehensive, integrated overview. The primary research questions for this theme are: 1) What are the main challenges that SPs face in their organizations?, and 2) How do these challenges interplay?

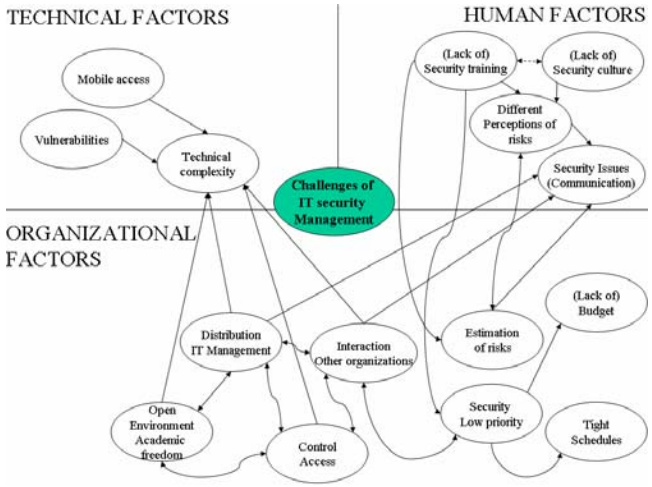

figure 3: Framework of the human, organization, and technological challenges impacting IT security management.

Prior research [6, 9, 13] has related organizational variables such as size, type of business, and top management support with security effectiveness, security culture, and enforcement of security policies within organizations. Our framework (figure 3) extends these with technological and human factors that interplay with each other and the organizational factors to directly impact ITSM. Finally, our findings highlight differences in challenges depending on the distributed and/or academic nature of the organization.

Impact of Security Management Model

One challenge we are investigating further is the organization's choice of security management model (SMM). A key tenet of SMM guidelines (e.g., CERT [7]), is that the security team include a manager who is centrally located within the organization. What is less clear is where to position the remaining SPs – there are tradeoffs with each SMM approach. We performed a

case study of 10 participants from one academic organization that recently disbanded a centralized security team in favour of a more distributed approach.

The case study revealed how challenging it is to implement a SMM that does not completely fit with organizational attributes. SMMs need to evolve along with the organization; SMM shifts are attempts to mitigate negative organizational traits (e.g., lack of authority) as well as to reflect current organizational goals. With each "swing" between SMMs, more and more prior security practices may be incorporated, in essence moving the SMM towards a hybrid model with attributes customized to and most fitting for the organization.

Security Responsibilities, Tasks, and Skills

Prior research studied security administrators and proposed directions for tool development [5]. The theme of security responsibilities, tasks, and skills takes a broader perspective, examining the ITSM workplace as a whole, including security practitioners with a wider range of duties.

As shown in figure 4, the responsibilities of security practitioners range from high-level design tasks such as *designing* security systems and developing policies and procedures, to investigative tasks such as *responding* to security incidents, to *maintenance* tasks such as updating access control lists [1]. We have also investigated the main tasks performed as well as three skill sets that are significant in ITSM: pattern recognition, inferential analysis including hypothesis generation and bricolage, and communication skills.

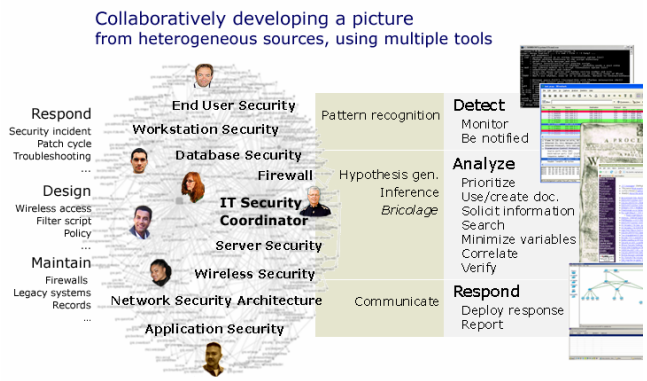

figure 4: The complex and collaborative environment of IT security management requires a variety of skills across a range of security activities and tasks.

Security incident response is still maturing as a field of practice [8]; and out investigations of this activity are ongoing (for preliminary results, see [14]). We are currently using the framework of challenges (figure 3) as a context for the tasks, strategies, skills, and tools used during response.

Collaborative Interactions

Security practitioners work in a distributed and collaborative environment, where communication breakdowns may create security vulnerabilities [1, 4, 5, 9]. Our goal in this theme is 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 collaboratively interact? 2) What tools do they need to interact?

Preliminary results identified eight collaborative security activities [15]. These represented a challenge for our participants, requiring different strategies to

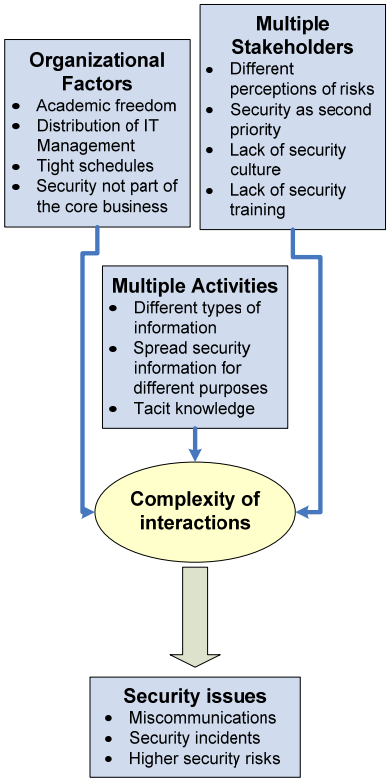

figure 5: Model of the factors and consequences of complex interactions in the context of IT security.

communicate security issues to stakeholders with different backgrounds and interests. This diversity also speaks to the complexity of interactions (figure 5). We have identified several opportunities for integrating security and communication tools.

Sub-optimal Situations in Distributed ITSM

The distributed and complex nature of ITSM often leads to sub-optimal or error situations. Busby [2] developed a framework for errors in a distributed system, and found that cues and norms were important for distributed cognition. For ITSM, we refine cues to include both information that is not intended as a directed communication and notifications; similarly, norms may be explicitly coded or be based on mutual understanding and transactive memory.

Analysis is still underway, but preliminary results indicate that ITSM relies heavily on broad tacit knowledge about technology and business, and transactive memory is used to activate that knowledge, especially when IT security must respond quickly to arising situations. Organizational complexity and change conspire against effective development and employment of transactive memory.

Implications of Results

Throughout our research themes, the complexity of IT security management has been a common thread. Our analysis suggests that the differences between security and general IT professionals 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 and manage diverse distributed tasks, while maintaining a deep and broad overview of the organization. The rich picture we are developing may serve as scenarios for those evaluating security tools [12]. For example, the analysis of collaborative interactions provides descriptions of communication and security tools used together; our sub-optimal situations theme describes instances where distributed cognition breaks down.

Each of our research themes has contributed to our understanding of this complex domain. As we have developed our models of the human, organizational, and technological factors which impact ITSM, we have grounded our work in other research domains. For example, security incident response shares many commonalities with both diagnostic systems and emergency management systems. Our investigation of sub-optimal situations applies distributed cognition theory and draws from knowledge management. While we learn from these other areas, we also can contribute rich descriptions of such systems in the ITSM domain.

Future Work

We will continue to develop our analysis of themes, in an effort to create testable models which may then be validated with larger populations. To that effect, we are currently refining a survey for the security challenges and collaborative interactions themes. Each theme has also resulted in a set of guidelines for improving tools and processes. We are currently working to incorporate these guidelines, comparing them with those derived in the related work to build a comprehensive framework for tools developed for security practitioners.

An open question remains of how to evaluate the success of tool refinements given the complex and distributed nature of ITSM. This is an active area of research within the domain of usability for complex

systems [12] and we hope that our efforts will provide methodological contributions.

Conclusions

In conclusion, we have presented the HOT Admin project, which investigates the work practices of IT security practitioners and the impact of human, organizational, and technological factors on these practices. Our goal is to develop better tools and processes for ITSM within organizations. Our research along six independent themes provides a timely contribution to this emerging field. We both validate and generalize prior work and extend knowledge of ITSM. We welcome collaborations with other researchers as we move from the field research phase to tool design, development, and evaluation.

Acknowledgements

Funding provided by the Canadian NSERC Strategic Partnership Program. Industry partners include SAP Labs Canada, Entrust, and Recombo. We thank the security practitioners who participated in our research.

References

[1] Botta, D., Werlinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S., and Fisher, B. *Towards Understanding IT Security Professionals and Their Tools*. Proc. of *Symposium on Usable Privacy and Security (SOUPS)*. ACM. (2007). 100-111.

[2] Busby, J.S., *Error and distributed cognition in design.* Design Studies, (2001). **22**: 233-254.

[3] Flechais, I. and Sasse, M.A., *Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science.* Int. J. Human-Computer Studies, (2007): doi:10.1016/j.ijhcs.2007.10.002.

[4] Haber, E. and Kandogan, E. *Security Administrators: A Breed Apart*. Proc. of *Workshop on Usable IT Security Management, SOUPS 2007*. (2007).

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

[6] Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., and Wei, K.-K., *An integrative study of information systems security effectiveness.* Int. J. Information Management, (2003). **23**(2): 139-154.

[7] Killcrece, G., Kossakowski, K.P., Ruefle, R., and Zajicek, M., *Organizational models for computer security incident response teams (CSIRTS)*. (2003): CMU/SEI-2003-HB-001 ADA421684: http://www.sei.cmu.edu/publications/documents/03.reports/03hb001.html.

[8] Killcrece, G., Kossakowski, K.P., Ruefle, R., and Zajicek, M., *Incident Management*. (2005): buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/incident/223.html.

[9] Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, F.N., *Managerial dimensions in information security: A theoretical model of organizational effectiveness*. (2005): www.isc2.org/download/auburnstudy2005.pdf.

[10] Kotulic, A.G. and Clark, J.G., *Why there aren't more information security research studies.* Information & Management, (2004). **41**(5): 597-607.

[11] Rayford, R.H., B. Vaughn, J., and Fox, K., *An empirical study of industrial security-engineering practices.* J. of Systems and Software, (2001). **61**: 225-232.

[12] Redish, J., *Expanding usability testing to evaluate complex systems.* J. Of Usability Studies, (2007). **2**(3): 102-111.

[13] Siegel, D.A., Reid, B., and Dray, S.M., *IT Security: Protecting Organizations in Spite of Themselves.* Interactions, (2006). **13**(3): 20-27.

[14] Werlinger, R. and Botta, D. *Detecting, analyzing, and responding to security incidents: A qualitative analysis*. Proc. of *Workshop on Usable IT Security Management (USM), SOUPS 2007*. (2007).

[15] Werlinger, R., Hawkey, K., and Beznosov, K. *Security Practitioners in Context: Their Activities and Interactions*. Proc. of *Ext. Abstracts of CHI 2008*. ACM. (In press).