Toward Understanding the Workplace of IT Security Practitioners

Konstantin (Kosta) Beznosov

Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
University of British Columbia
IT Security is Critical
IT Security is Costly

organizations worldwide spent in 2007

$1.55 trillion on IT
7-9% on IT security

$108 billion

Forrester Research

Cyber crime market worldwide

$105 billion

John Viega, McAfee
Outline

• overview
• methods
• results
  • tasks & tools
  • IT security vs. general IT
  • challenges
  • interactions
• opportunities for future research
HOT Admin:
Human Organization and Technology Centred Improvement of IT Security Administration

Purpose

- **Tool evaluation**: methodology
- **Tool design**: guidelines & techniques

Work Plan

- **Field study**
- **Models**
- **Techniques & Methodologies**
- **Validation & Evaluation**

**sponsors and partners**

- **Entrust**
- **NSERC CRSG**
- **SAP**
Human Organization and Technology Centred

Human

Organizational

Technological

hotadmin.org
Outline

• overview
• methods
• results
  • tasks & tools
  • IT security vs. general IT
  • challenges
  • interactions
• opportunities for future research
Methods Summary

• data collection
  • online questionnaire
    • demographics
  • in situ semi-structured interviews
    • two interviewers
  • participatory observations
    • 75 hours in academic organization IT department
    • policy development and IDS deployment

• data analysis
  • qualitative description
    • constant comparison, inductive analysis
    • coding: selective, open, axial, theoretical
Interviewer:

*Do you think that there's a difference between security-related tasks and other IT tasks? Can you talk about what makes security different?*

Participant:

Well a very glib answer would be that they are different because security involves making things more difficult for people rather than not. Like I said, that's a glib answer and not necessarily completely true but the element of truth in that is that typically if there is a security problem, the solution is to get people to stop doing that - whatever it might be. If someone wants to run a file-sharing program on the computer - well, no, don't do it because it opens us up to X Y and Z. That leaves them bored and frustrated. Or, don't go to that website, well but like I said those are very glib answers and only cover certain cases where you are telling people don't do the thing that involves exposing us to problems.

A lot of the time the other IT stuff, the non-security related IT stuff tends to be helping people get their work done in a more or less immediately visible way. I can't get my e-mail or, here's how. I can't print, here's how. Checking mail this way sucks. Well let me take three months and get a good web mail program. The server went down for the third time today, okay; let me spend three months getting a better server and redundant servers and things like this.
"...I do my own risk assessment for everything I've responsible for. Unfortunately in my opinion not enough people understand risk management."

"in my experience these are some of the things that can happen and these are some of the potential situations you'll have to deal with"

"The security coordinators take it to the data guardian and explain what the risks are."

<table>
<thead>
<tr>
<th>Stories from interviews</th>
<th>open codes</th>
<th>axial codes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal assessment of risk</td>
<td>Different perceptions of risk</td>
</tr>
<tr>
<td></td>
<td>People do not understand risk management</td>
<td>Memos: ideas, relationships</td>
</tr>
<tr>
<td></td>
<td>Explain security risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain security risks</td>
<td></td>
</tr>
</tbody>
</table>

Memos: ideas, relationships
recruitment

challenges
• overworked
• secrecy culture
• backstage

approaches
• professional contacts
• practical benefits
• gradual recruitment
• gatekeepers

“Hello... I’m sorry but I must decline this opportunity. We don’t discuss our security administration with anyone other than with the owners of the resources we’re securing.”

IT security manager who declined access to his department

34 interviews with 36 participants between July 2006 and March 2008
Industry Sectors

34 interviews

16 organizations

- Academic
- Finance
- Insurance
- Scientific services
- Manufacturing
- Retail/Wholesale
- Government Agency
- Telecommunications
- Non-for-profit Organization
- High-Tech
- IT Consulting
Job Types

- IT Manager: 5
- Security Manager: 5
- Security Specialist: 11
- IT (with security tasks): 14

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
Analysis Themes

- tasks & tools
- IT security vs. general IT
- challenges
- interactions
- sub-optimal situations
- management model
Outline

• project overview
• methods
• results
  • tasks & tools
  • IT security vs. general IT
  • challenges
  • interactions
• opportunities for future research
theme: tasks and tools

tasks & tools

IT security vs. general IT

challenges

interactions

sub-optimal situations

management model

André Gagné

David Botta

Rodrigo Werlinger

André Gagné
findings: no security admins!

- system analysts
- application analysts
- business analysts
- technical analysts
- system administrators
- application programmers
- auditors
- IT managers
- security leads
- network leads

```
"... what makes me [a security] analyst is that I'm also involved in developing the policies and procedures ... an analyst is also someone who's doing a certain amount of troubleshooting and someone who's, I guess, a little bit more portable in terms of what their daily responsibilities are going to be like."
```
findings: loosely coordinated teams

“I have a security team that I work with. They don’t report to me but I actually work with them and they sort of are represented by the different areas.”

study participant

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
findings: main kinds of responsibilities

maintain
• firewalls
• legacy systems
• records
• ...

respond
• security incident
• patch cycle
• troubleshooting
• ...

design
• wireless access
• filter script
• application security architecture
• ...

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
findings: activity chain

- Monitor
- Be notified
- Prioritize
- Use/create documentation
- Solicit information
- Search
- Analyze
- Correlate
- Verify
- Choose/deploy response
- Report

So what?
- interdependence of activities
- just-in-time decision making
findings: skills

• pattern recognition
• inferential analysis
• use of tacit knowledge
• bricolage

So what?
• finding gaps in tool support
• tool improvement
• new usability testing methods

- Dictionary: “construction or creation from a diverse range of available things”
- Origin: mid 20th century: French, from bricoler ‘do odd jobs, repair.’

for more information

theme: IT security vs. general IT

- tasks & tools
- IT security vs. general IT
- challenges
- interactions
- sub-optimal situations
- management model

André Gagné
Kasia Muldner
Differences Along Five Dimensions

Scope

Troubleshooting Complexity

Usability vs. Security Tradeoff

Fast-paced Environment

Negative Stakeholder Perception
Usability vs. Security

security practitioners are constantly balancing usability and security

“I think it [security and general IT] is different because you have to balance the usability of the system with its 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”

study participant

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
Perception and Environment

• Perception by stakeholders
  • Security practitioners (SPs) are perceived in a less positive light by organizational stakeholders

• Fast-paced technological environment
  “IT is a fast changing field and security is even faster”
  • (Only) SPs have to contend with active and continuous threats
Need for Broader Scope

SPs need broader internal scope than general IT

"... 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"

study participant

SPs need broader external scope than general IT

Legislation (e.g., Sarbanes Oxley)
Model of Differences

Reality of Security

Usability vs. Security Tradeoff

Troubleshooting Complexity

Fast-paced Environment

Response Time

Need to be up to Date

Persuasion Tactics

Negative Stakeholder Perception

Scope

For more information:
so what?

• Reduce troubleshooting complexity
  • Tools supporting distributed nature of IT security
  • Tools for making tacit knowledge explicit

• Influence stakeholder perception
  • Via management buy in [Siegel et al. 2006]

• Mitigate need for usability-vs-security tradeoff
  • Shift in design culture [Smetter & Grinter 2002]
  • Stakeholder involvement during design process [Flechais & Sasse 2007]
Related work has studied challenges in isolation

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
Challenges: Technological

• Vulnerabilities
• System Complexity
  • A typical network could have firewalls, DMZs, proxies, switches behind the firewall, routers in front of the firewalls, mail servers and not enough people to look after the overall security of these interconnected devices
• Mobile Access
  • Mobile user access makes it challenging to secure resources
Challenges: Human

- Security Culture
  - Poor security practices result in difficulties to implement security controls

- Training
  - SPs lack the necessary training

- Communication
  - Difficulties for SP’s to communicate risks and security issues due to the lack of common view among stakeholders
Challenges: Organizational

- **Risk Assessment**: Difficult to estimate IT security risks.
- **Business Relationships**: Misaligned security policies make it challenging to enforce standards within an organization.
- **Security Low Priority**: Security is not a priority for many stakeholders.
- **Task Distribution**: Distribution of responsibilities was an issue: “the decentralized nature does not help”...
- **Open Environment**
- **Tight Schedules**
- **Data Access**
- **Budget**
Theme: Interactions

- tasks & tools
- IT security vs. general IT
- challenges
- interactions
- sub-optimal situations
- management model
Analyzed Interactions

1. performing security audits
2. defining security requirements for new projects
3. solving end-user security issues
4. implementing security controls
5. training and educating other specialists
6. mitigating new vulnerabilities
7. developing security policies
8. responding to security incidents
Interactions During Incident Response

Security practitioners (SP)
- Respond to security incident
  - Discussion of next steps
  - Notification

Managers
- Coordinate next steps during the investigation
- Ask SP to take action on alarms
  - Requirements

External IT organizations
- ISPs/ICP administration
  - Monitor Internet
  - Provide security consultancy
- Share security knowledge (community of practice)
  - Notifications

IT specialists
- Administrate network or systems
- Administrate data bases
- Forward alarms
  - Requirements
  - Analysis of the incident

End-Users
- Experience security incident
  - Suspect of a security incident
  - Requirements

Other Stakeholders
- Redefine product
  - Contact clients or end-users
  - Revise contracts with customers
  - Discussion of action plan
  - Notifications

Notifications

Requirements

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
so what?

- how integrate information from different communication channels
- how provide customizable account structure
- how adapt reports to the recipient


Putting It All Together

- Complexity of IT security management
- Understanding of IT security professionals
- Guidelines for tool refinements and directions for future research
What We Are Busy With Now

- how sub-optimal situations arise
- design guidelines
- tool evaluation framework
Opportunities for Future Research

• Creating testable models for validating and extending findings?

• Transforming guidelines into concrete tool refinements?

• Evaluating tools refinements given the complex and distributed nature of IT security?
Selected Project Publications


