Security practitioners in context:

Their activities and collaborative interactions

Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov

Department of Electrical and Computer Engineering
University of British Columbia

Motivation

Security tasks are highly interdependent.

To improve security tools, we need to understand how security practitioners collaborate in their organizations.

Approach

Field Study Goals

Security practitioners:

- What do they do?
- With whom do they interact?
- How do they interact?

Data collection

- Semi-structured interviews
- Questionnaires
- Participatory observation

Analysis

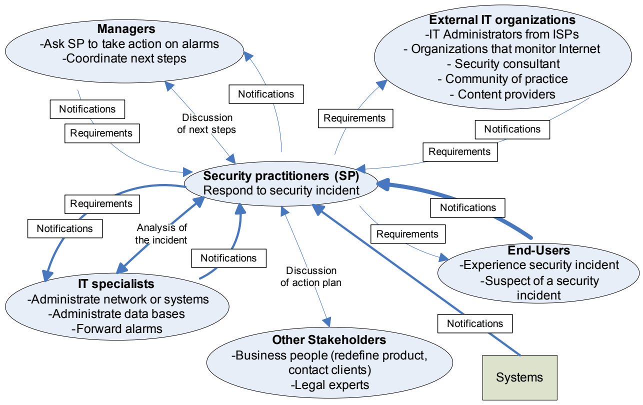
- Identify interactions
- Identify resources used during interactions
- Propose improvements of security tools and practices

Results

Security practitioners perform many activities:

- Security audits
- Train and educate other specialists
- Design new IT services including security criteria
- Mitigate new vulnerabilities
- Solve end-users IT security issues
- Develop security policies
- Implement access security controls
- Respond to security incidents

Each activity involves information exchange with multiple stakeholders:



Managers
-Ask SP to take action on alarms
-Coordinate next steps

External IT organizations
-IT Administrators from ISPs
- Organizations that monitor Internet
- Security consultant
- Community of practice
- Content providers

Security practitioners (SP)
Respond to security incident

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

IT specialists
-Administrate network or systems
-Administrate data bases
-Forward alarms

Other Stakeholders
-Business people (redefine product, contact clients)
-Legal experts

Systems

Notifications

Requirements

Discussion of next steps

Notifications

Requirements

Notifications

Requirements

Requirements

Notifications

Analysis of the incident

Notifications

Discussion of action plan

Notifications

Requirements

Notifications

Example: five different stakeholders to respond to security incidents

Diverse, Customized Exchange of Information

- Information exchanged in different formats across multiple communication channels
- Security information spread for different purposes:
  - Report
  - Notification
  - Requirement
- Use of tacit knowledge

Organizational Factors

- Academic freedom
- Distribution of IT management
- Tight schedules
- Security not part of the core business

Multiple Stakeholders Involved

- Different perceptions of risks
- Security as second priority
- Lack of security culture
- Lack of security training
- Transactive memory

Complex Interactions → **Security Issues**

hotadmin.org

Implications for Research

Develop security tools that:

- Integrate information from different communication channels
- Provide flexible reporting (reports adapted to the recipient)
- Communicate security information between secure and insecure domains
- Integrate unrelated databases
- Communicate configuration changes (e.g., firewalls)
- Provide customizable account structure