



# 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

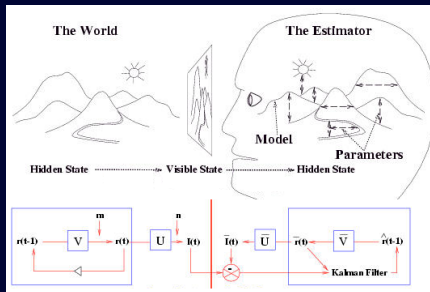
## Purpose

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

## Work Plan



Field study



Models



Techniques &  
Methodologies



Validation & Evaluation

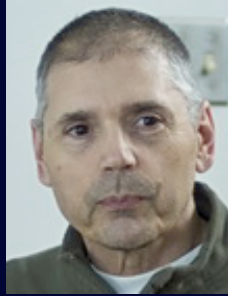
sponsors and  
partners



# Project Team



**Kosta Beznosov**



**David Botta**



**Rodrigo Werlinger**



**Kirstie Hawkey**



**Kasia Muldner**



**Brian Fisher**



**Pooya Jaferian**



**Fahimeh Raja**



**Lee Iverson**



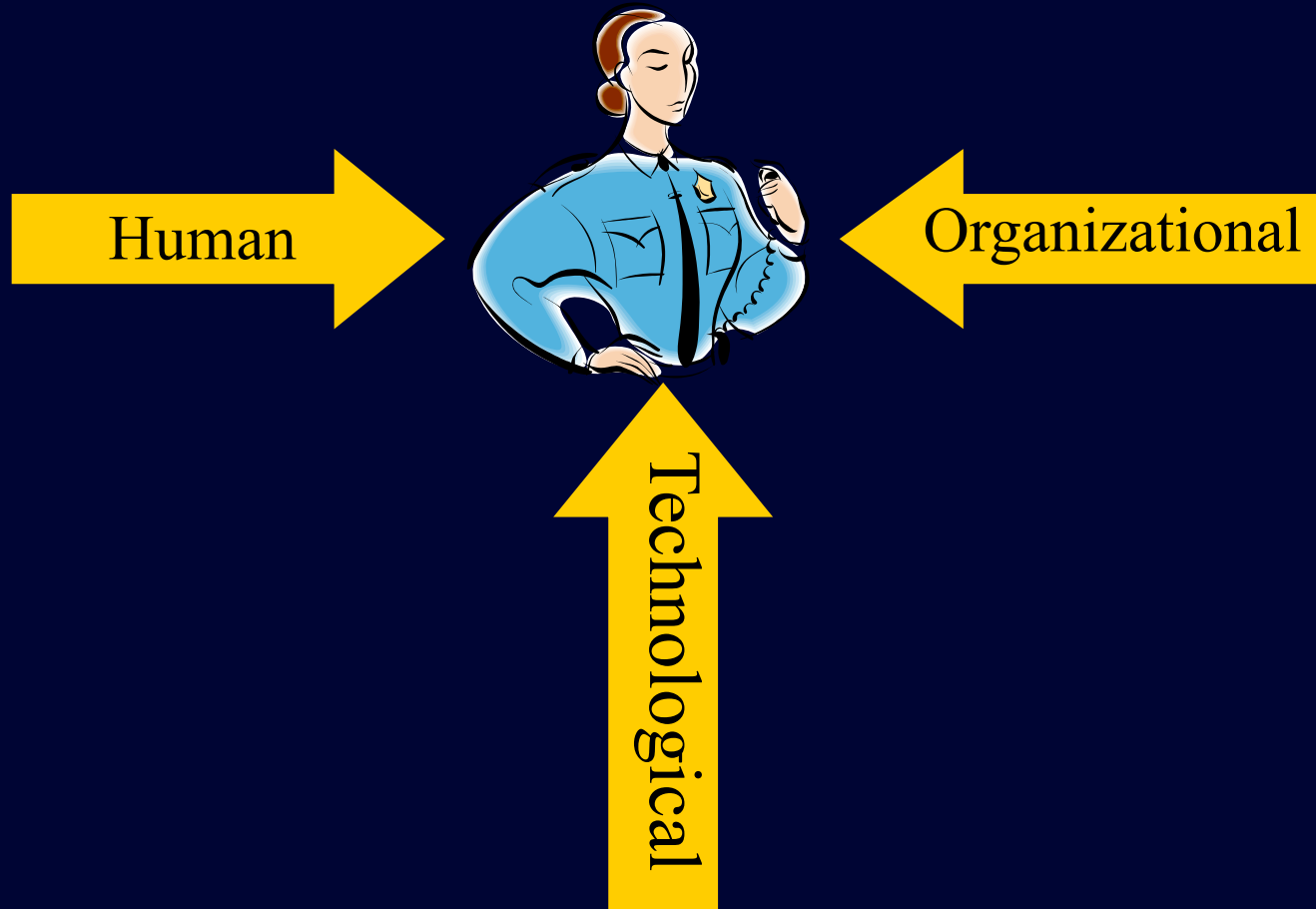
**André Gagné**



**Sid Fels**



# Human Organization and Technology Centred



hotadmin.org

**hotadmin.org**

Here are some related websites for: hotadmin.org

Search

#### Sponsored Links

##### Claims Administration

Learn about the challenges and how technology can help you  
[www.ClaimVantage.com](http://www.ClaimVantage.com)

##### Simplify & Centralize Win

Management tasks are centralized and made simple. Great Admin Tool!  
[www.softwareshefdistribution.com](http://www.softwareshefdistribution.com)

##### Hot Babes In Your Bed

Loneliness Sucks - Fill Your Life With Hot Babes. Video Example!  
[www.PickUp101.com](http://www.PickUp101.com)

##### Filipinas look for love

Pretty girls from Philippines look for serious relation worldwide  
[www.filipinokisses.com](http://www.filipinokisses.com)

##### Sexy Russian Babe

Find a Hot Russian Babe Online E-mail Amazing Girls Today!  
[www.Anastasiaweb.com](http://www.Anastasiaweb.com)

##### Third Party Verification

Automated or Live Agent Turn-key, No Capital Costs  
[www.intelemedia.com](http://www.intelemedia.com)

##### Red Hot Deals

Update your fall look for less with sweet deals on sexy red boots  
[www.personalshopper.com](http://www.personalshopper.com)

##### Sizing Guide for MySQL

Free Sizing Guide and Performance Benchmarks for MySQL on Blade  
[www.mysql.com](http://www.mysql.com)

##### Sexy women, jt tinney

jt tinney bikini girls stacey hayes Playboy Model Louise Glover, babes  
[www.knockoutmag.com](http://www.knockoutmag.com)

#### Related Categories

[Hot Blonde](#)

[Hot Bra](#)

[Hot Celebrities](#)

[Hot Clothing](#)

[Hot Ladies](#)

[Hot Legs](#)

[Hot Swimsuit](#)

[Hot Wallpapers](#)

[Hot Asian](#)

[Hot Cup](#)



# 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

# coding example

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 that because it opens us up to X Y and Z. That leaves the user frustrated. Or, don't go to that website, well but that's like I said those are very glib answers and only cover 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 to get a better mail program. The server went down for the third time, let me spend three months getting a better server. Servers and things like this.

Security hinders users

Security vs.  
Usability

IT helps users

# another coding example

## Stories from interviews

## open codes

## axial codes

"...I do my own risk assessment for everything I've responsible for. Unfortunately in my opinion not enough people understand risk management."

Personal assessment of risk

People do not 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"

Explain security risks

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

Explain security risks

Different perceptions of risk



Memos: ideas, relationships

# recruitment

## challenges

- overworked
- secrecy culture
- backstage

## approaches

- professional contacts
- practical benefits
- gradual recruitment
- gatekeepers

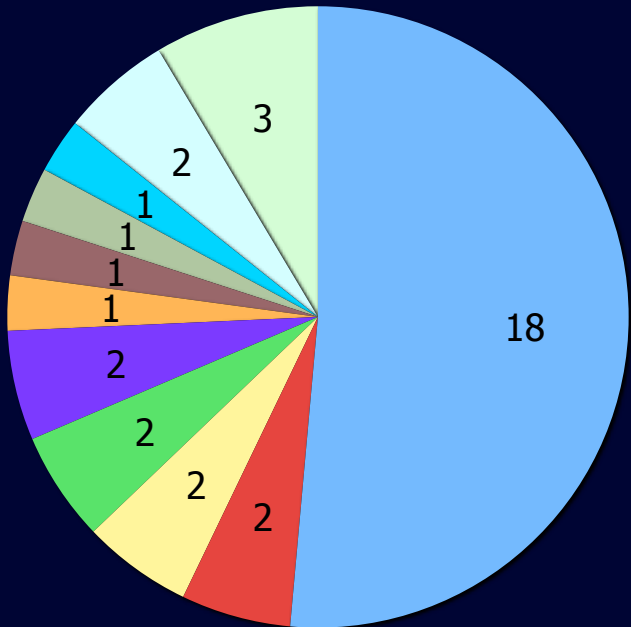
*“Hello... I’m sorry but I must decline this opportunity. We don’t discuss our security administration with anyone other than with the owners of the resources we’re securing.”*

IT security manager who declined access to his department

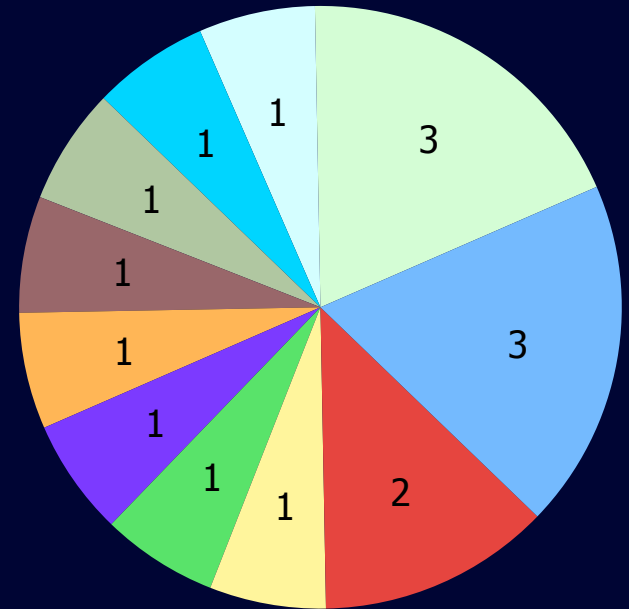
**34 interviews with 36 participants  
between July 2006 and March 2008**

# Industry Sectors

34 interviews

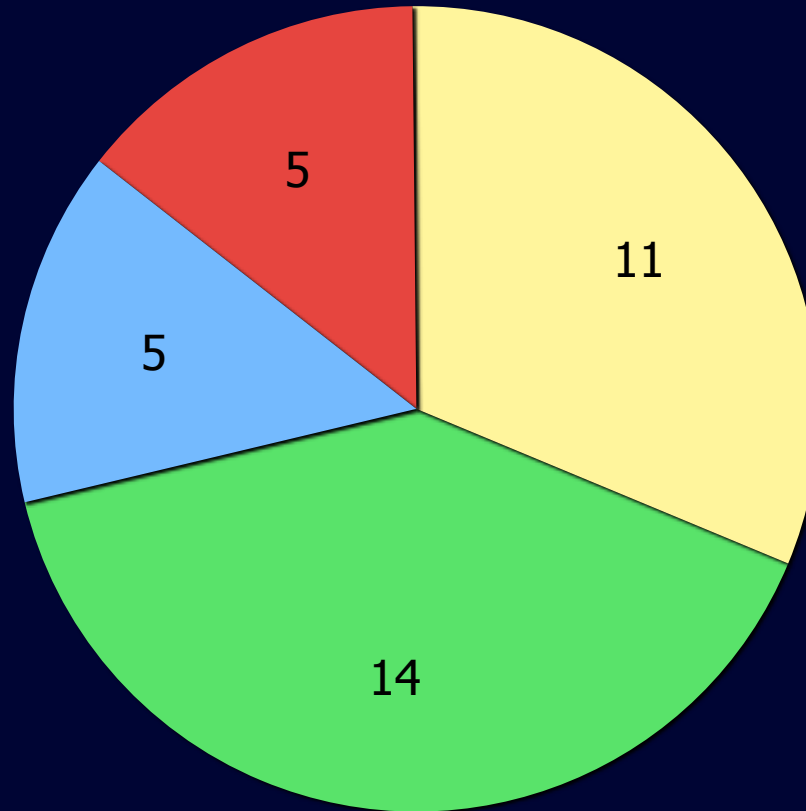


16 organizations



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

# Job Types



- IT Manager
- Security Manager
- Security Specialist
- IT (with security tasks)

# 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

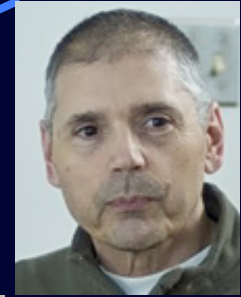
IT security vs. general IT

challenges

interactions

sub-optimal situations

management model



**David  
Botta**



**Rodrigo  
Werlinger**



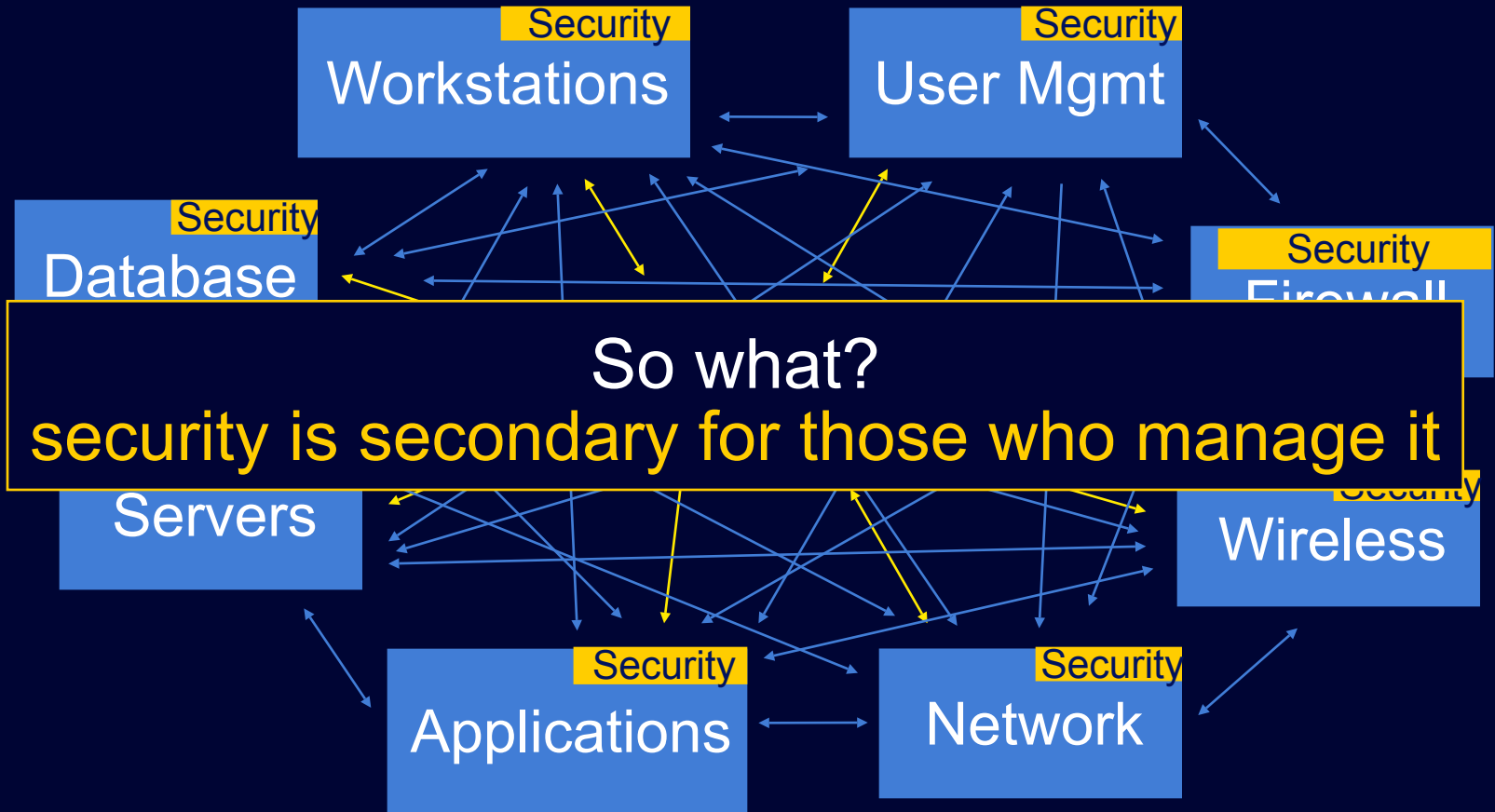
**André  
Gagné**

# 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<sub>H</sub>

# findings: main kinds of responsibilities

## maintain

- firewalls
- legacy systems
- records
- ...

## respond

- security incident
- patch cycle
- troubleshooting
- ...

## design

- wireless access
- filter script
- application security architecture
- ...

# 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

D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, “Towards understanding IT security professionals and their tools,” in the *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pp. 100-111, Pittsburgh, PA, July 18-20 2007.

# 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



# 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

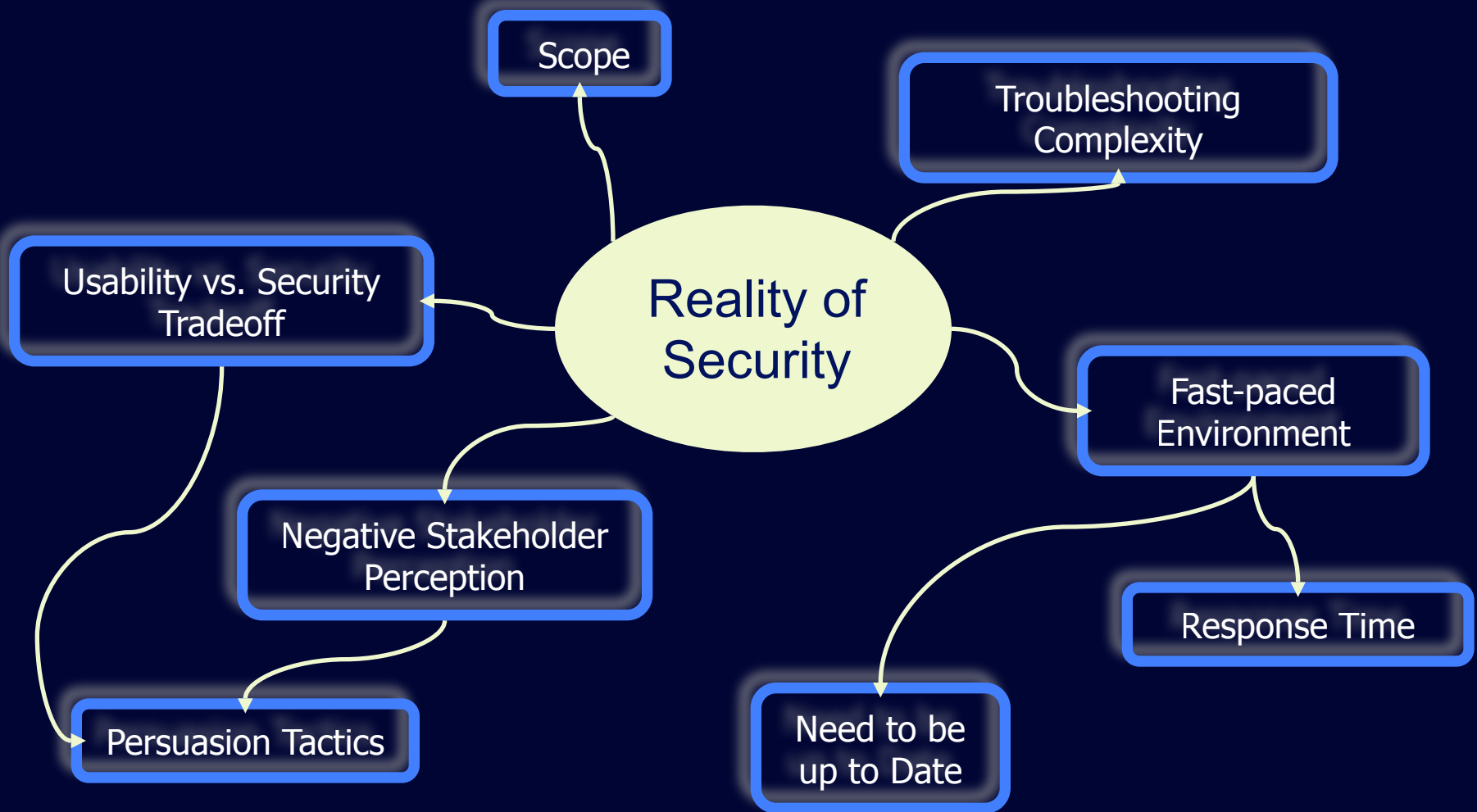
*"... you really need to be able to look quite wide and deep. You need to be able to **look within the packet** in a lot of detail to understand how an intrusion detection system works... And at the same time you need to take **a wide look to an organization** to be able to determine ... the risks... 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



For more information:

A. Gagné, K. Muldner, K. Beznosov, "**Identifying Security Professionals' Needs: a Qualitative Analysis**", to appear in the Proceedings of the *Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.

# 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]

# Theme: Challenges

tasks & tools

IT security vs. general IT

challenges

interactions

sub-optimal situations

management model



**Rodrigo Werlinger**

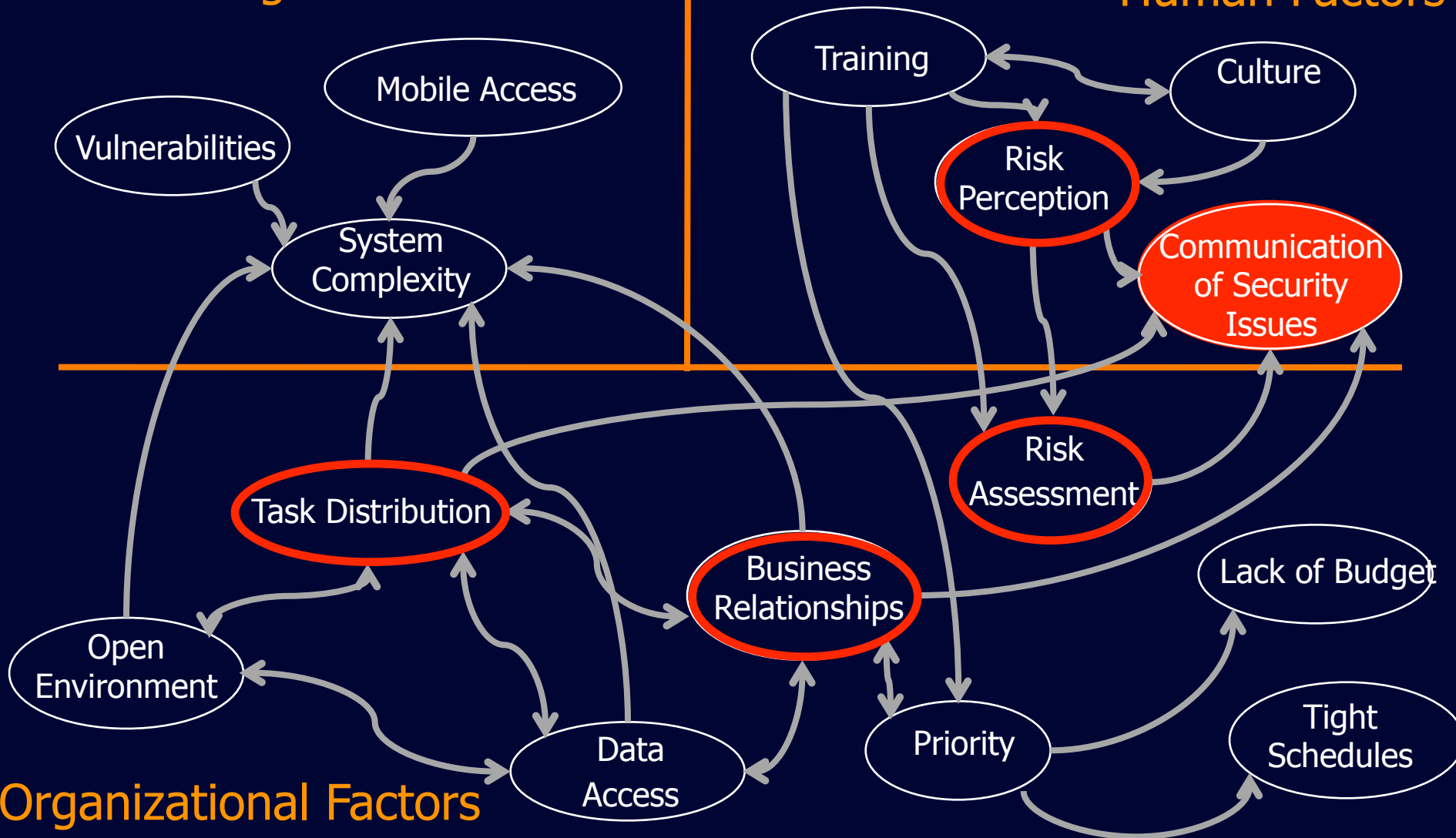


**Kirstie Hawkey**

Related work has studied challenges in isolation

# Technological Factors

# Human Factors



R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.



# 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



**Rodrigo Werlinger**

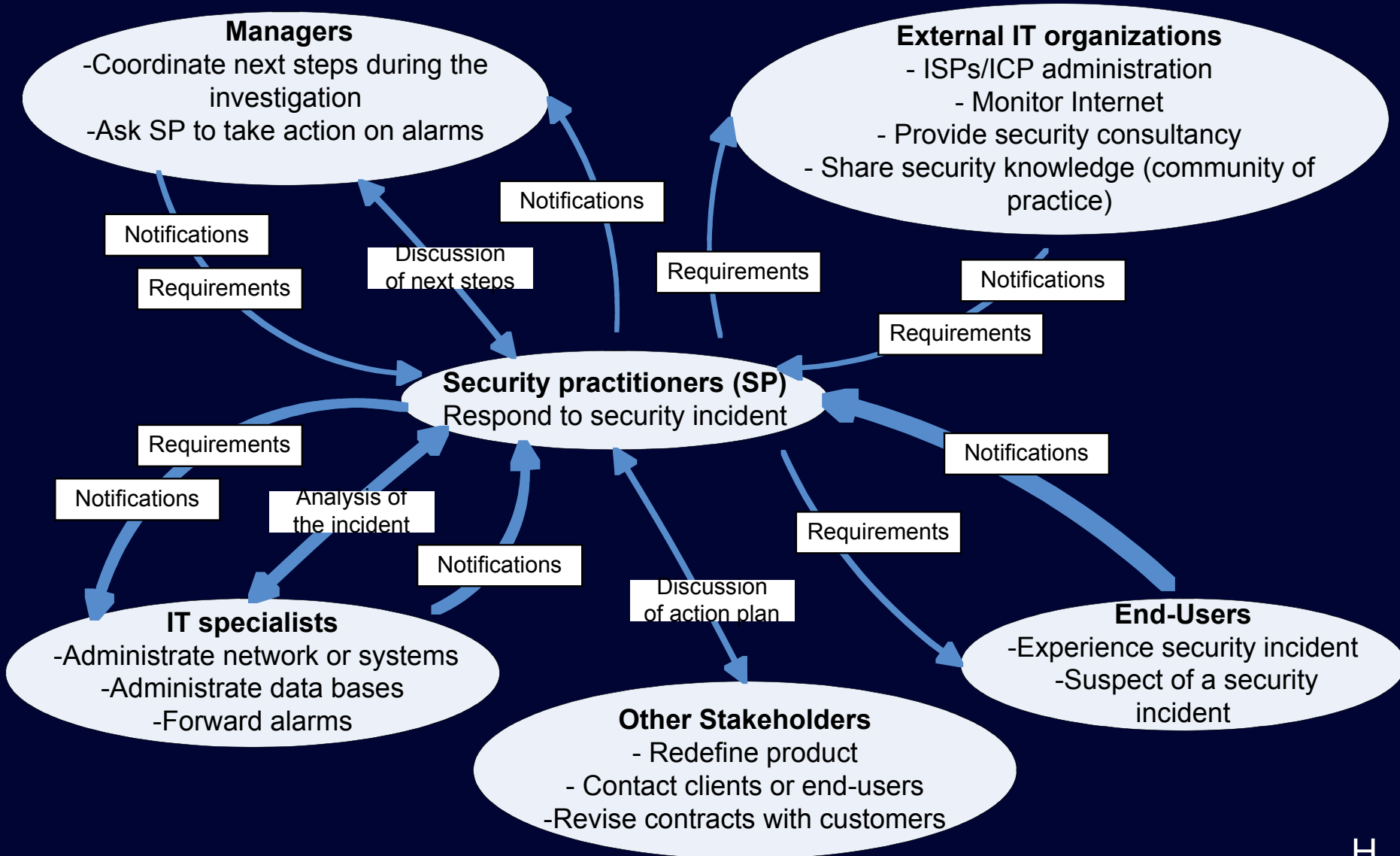


**Kirstie Hawkey**

# Analyzed Interactions

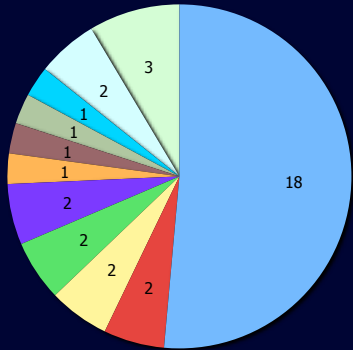
1. performing security audits
2. defining security requirements for new projects
3. solving end-user security issues
4. implementing security controls
5. training and educating other specialists
6. mitigating new vulnerabilities
7. developing security policies
8. responding to security incidents

# Interactions During Incident Response

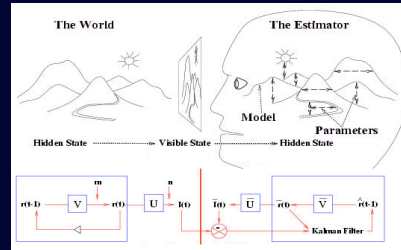


# so what?

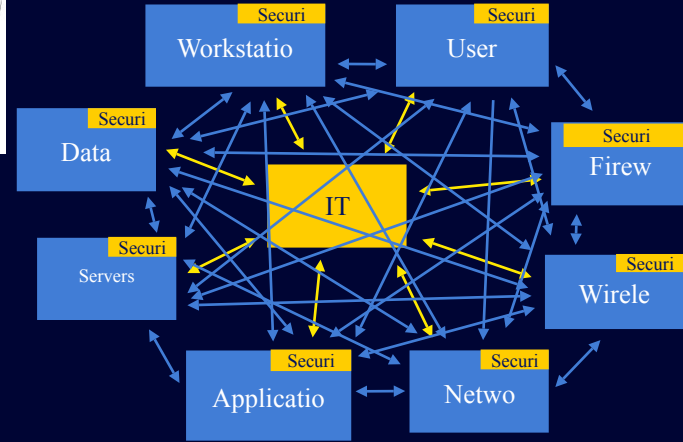
- how integrate information from different communication channels
  - how provide customizable account structure
  - how adapt reports to the recipient
- 
- R. Werlinger, K. Hawkey, K. Beznosov “**Security practitioners in context: Their activities and collaborative interactions**” presented at *Work in Progress poster session of the ACM SIG CHI conference*, April 5-10, 2008, Florence, Italy.
  - R. Werlinger, K. Hawkey, K. Beznosov, “**Security practitioners in context: Their activities and interactions with other stakeholders within organizations,**” under review.



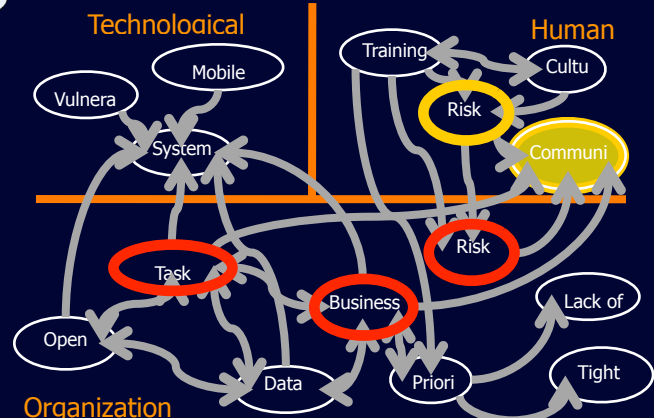
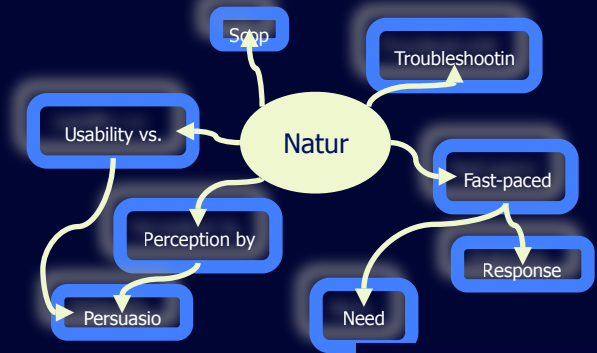
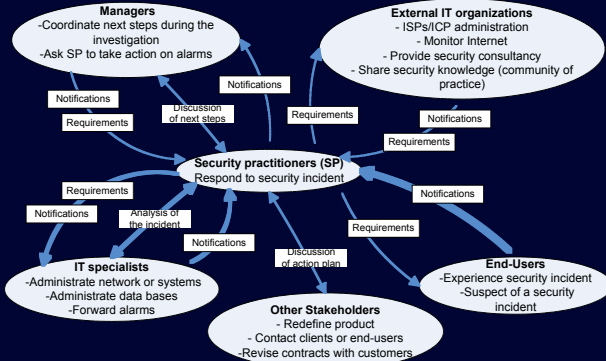
Field study



Models



# H O A T





# 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

- R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, K. Beznosov “**The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?**” to appear in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Carnegie Mellon University, Pittsburgh, PA, USA, 23-25 July 2008.
- A. Gagné, K. Muldner, K. Beznosov, “**Identifying Security Professionals' Needs: a Qualitative Analysis**”, to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.
- R. Werlinger, K. Hawkey, K. Beznosov, “**Human, Organizational and Technological Challenges of Implementing IT Security in Organizations**”, to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.
- K. Hawkey, K. Muldner, K. Beznosov, “**Searching for the Right Fit: A case study of IT Security Management Models**,” in *IEEE Internet Computing Magazine*, May/June 2008.
- K. Beznosov and O. Beznosova, “**On the Imbalance of the Security Problem Space and its Expected Consequences**,” *Journal of Information Management & Computer Security*, Emerald, vol. 15 n.5, September 2007, pp.420-431.
- D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, “**Towards understanding IT security professionals and their tools**,” in the *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pp. 100-111, Pittsburgh, PA, July 18-20 2007.