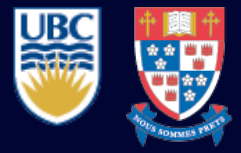


HOT Admin Research Project

Overview and Results to Date

Konstantin (Kosta) Beznosov
University of British Columbia

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 Expensive

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

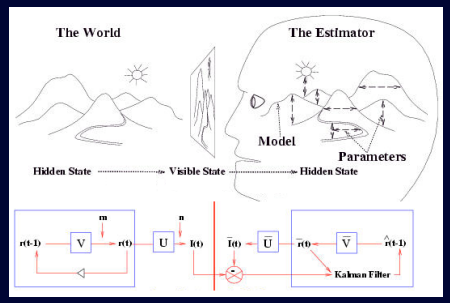
- HOT Admin project
- How we do the study
- What we got

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

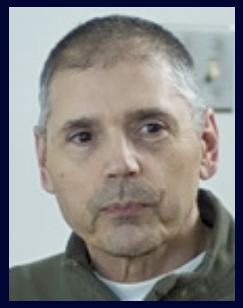
Entrust

NSERC CRSNG

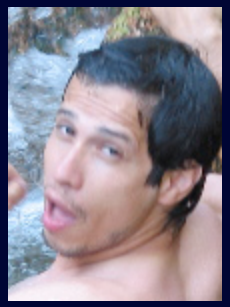
SAP

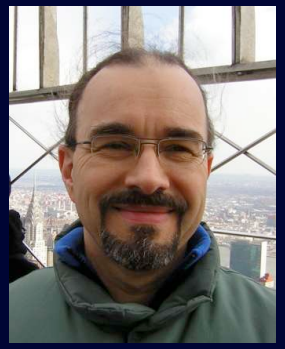
Project Team

Dr. Konstantin Beznosov
- Principal investigator (PI)
- Assist. Prof., ECE, UBC
- security; 5 years of industry



Dr. Sidney Fels
- Assoc. Prof., ECE, UBC
- new interfaces design

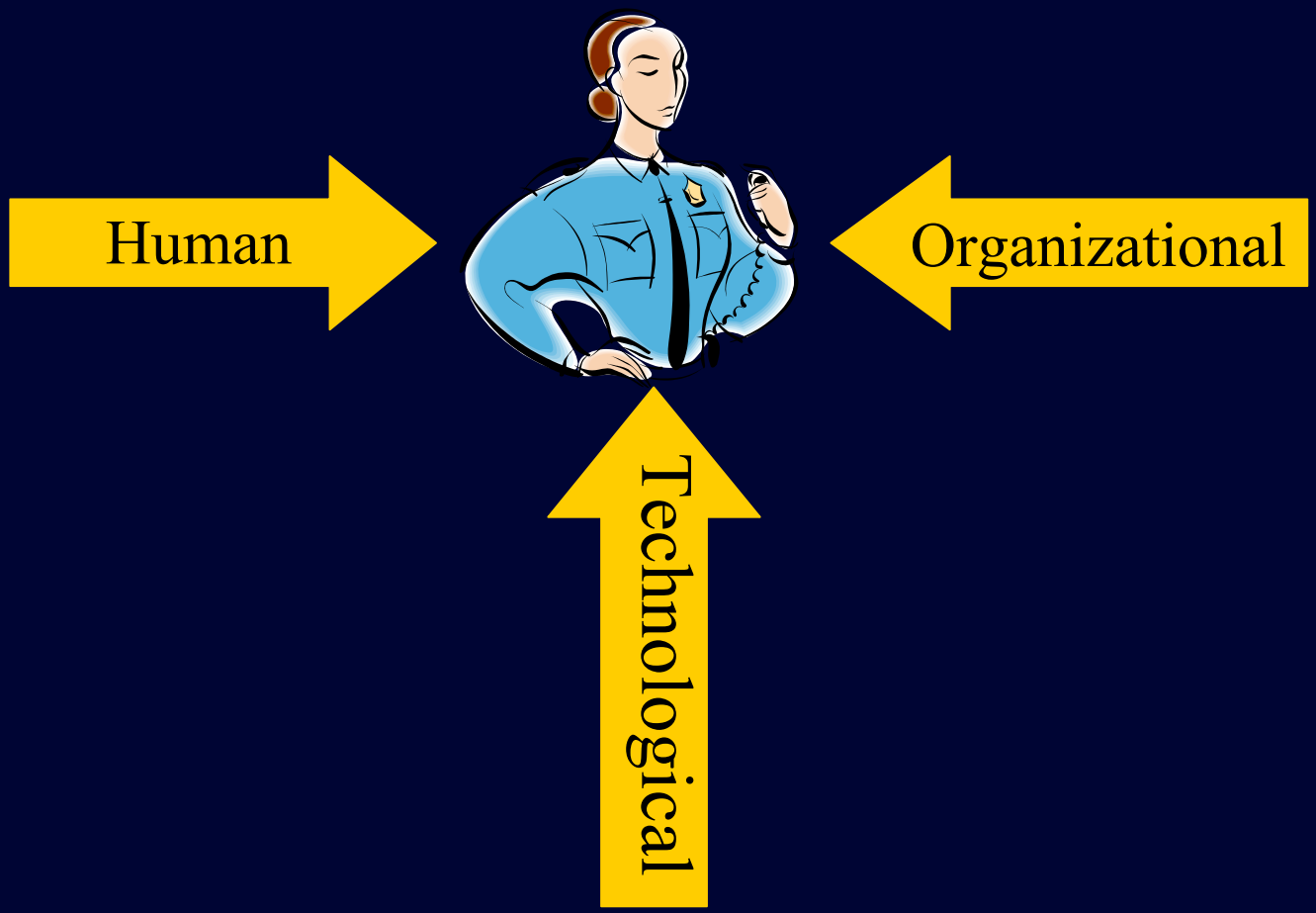




Dr. Lee Iverson
- Assist. Prof., ECE, UBC
- Inform. visualiz.
- collaboration infrastructures

Dr. Brian Fisher
- Assoc. Prof. of Inter. Arts and Techn., SFU
- Adjunct Prof. in MIS and CS, UBC
- cognitive science-based interaction design

Human **O**rganization and **T**echnology Centred



hotadmin.org

Methods

Recruitment

Challenges

- Overworked
- Secrecy culture
- Backstage

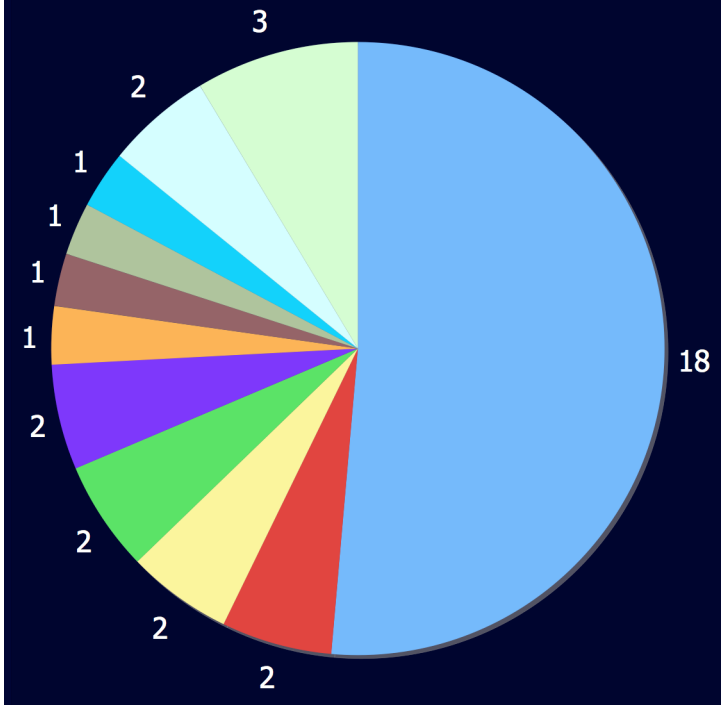
Approaches

- Professional contacts
- Practical benefits
- Gradual recruitment
- Gatekeepers

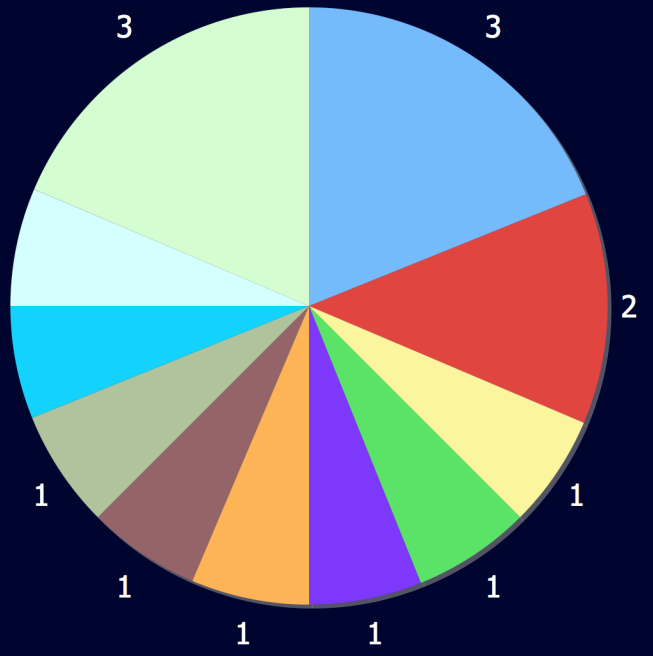
As of January 2008, 33 interviews with 35 participants

Industry Sectors

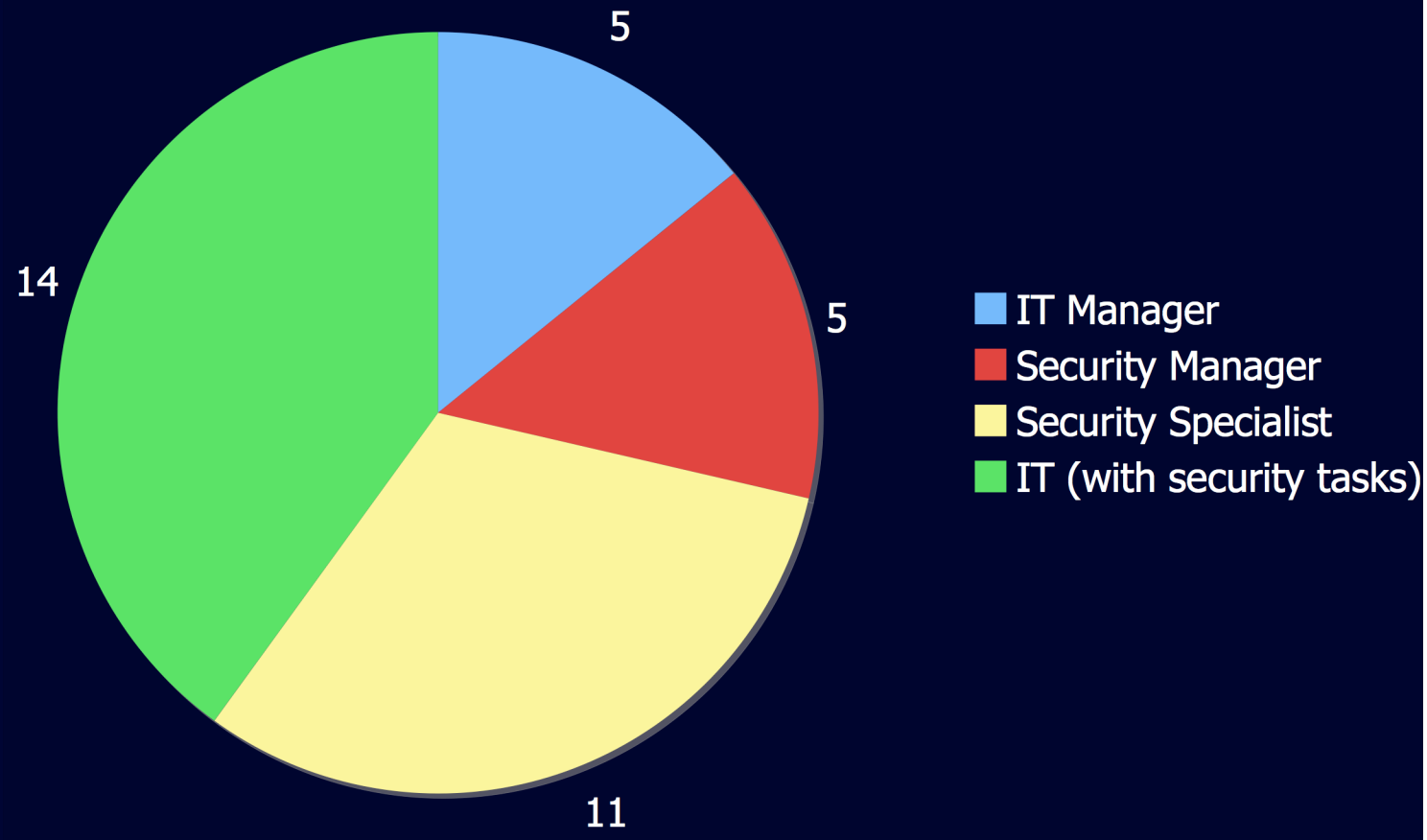
participants



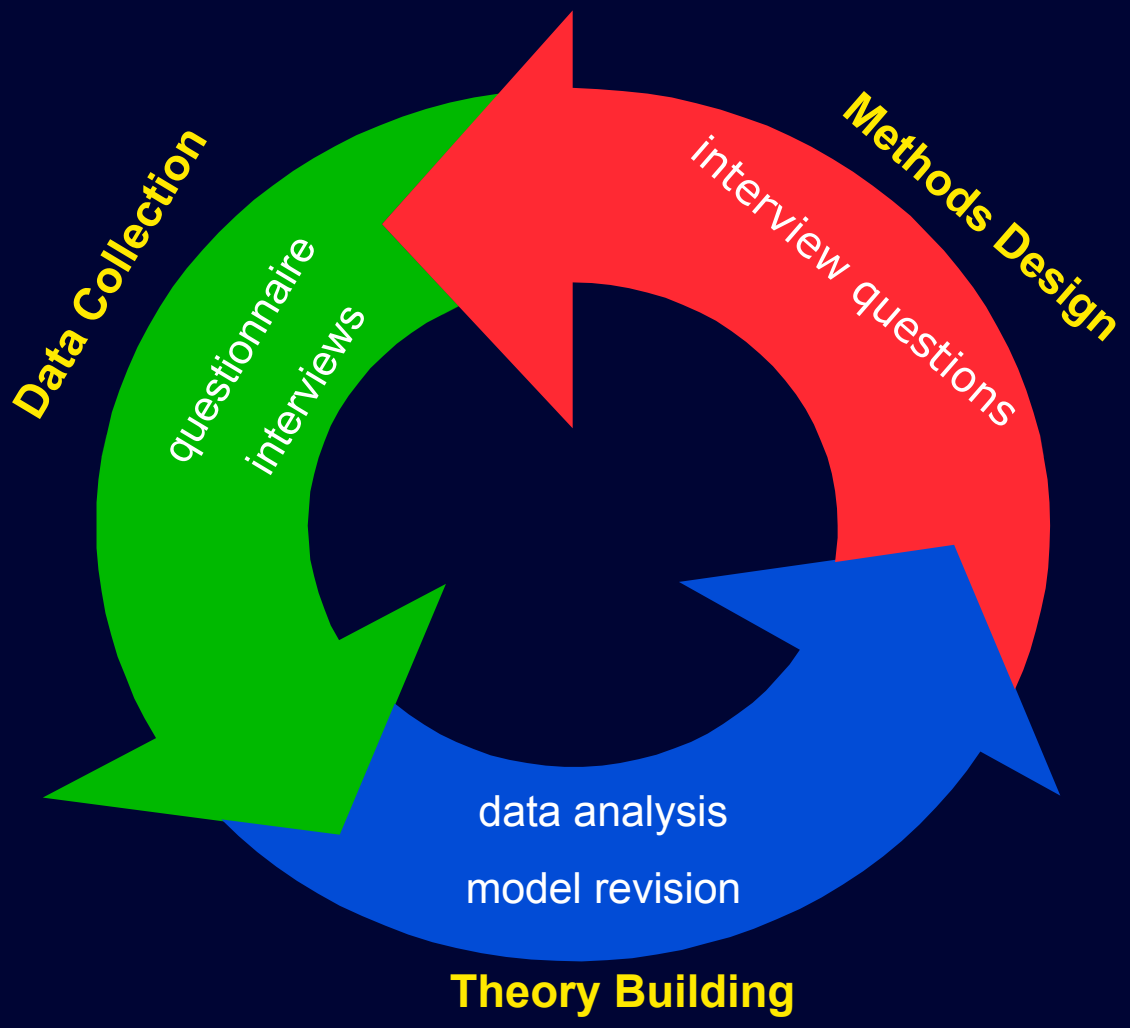
participated organizations



Job Types


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

Analysis


Data Collection
questionnaire
interviews
Methods Design
interview questions
data analysis
model revision
Theory Building

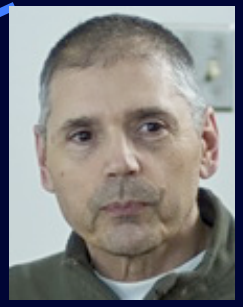
Analysis Themes

- Tasks & Tools
- IT Security vs. General IT
- Challenges
- Interactions
- Errors
- Management Model

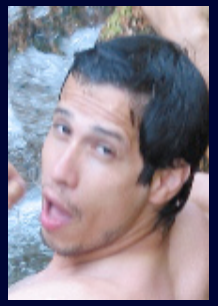
Results

Theme: Tasks and Tools

- Tasks & Tools
- IT Security vs. General IT
- Challenges
- Interactions
- Errors
- Management Model



David Botta



Rodrigo Werlinger

André Gagné

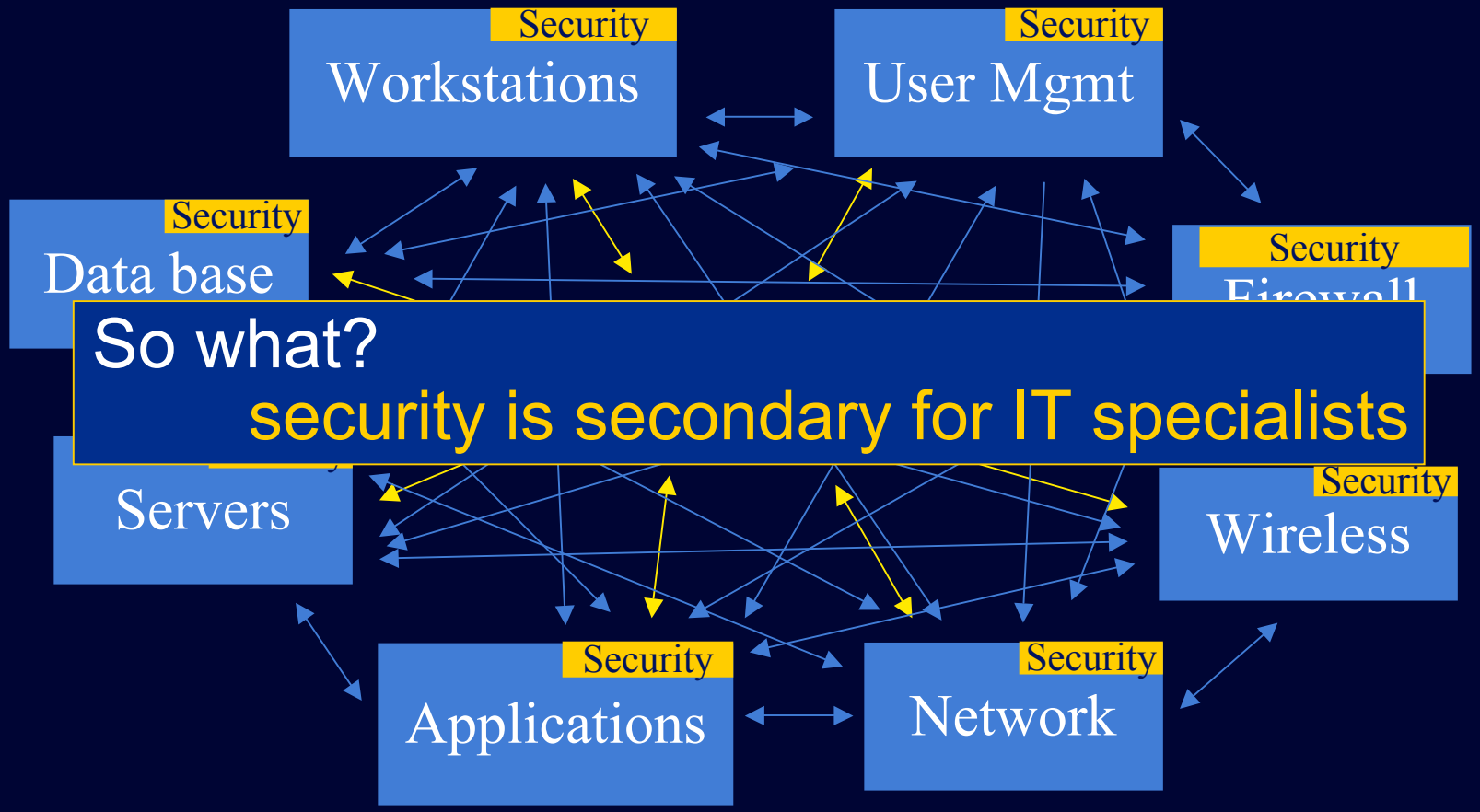
No Security Admins!

- 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*."

Study Participant

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

Three Main Kinds of Responsibilities

Respond

- Security incident
- Patch cycle
- Troubleshooting
- …

Design

- Wireless access
- Filter script
- Application security architecture
- …

Maintain

- Firewalls
- Legacy systems
- Records
- …

So what?

disjoint responsibilities → fosters distributed security teams requires tool support

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
- deployment of
  - resources
  - knowledge
  - skills

Skills

- Pattern recognition
- Inferential analysis
- Bricolage
- Tacit knowledge

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

- 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
- Errors
- Management Model

André Gagné

Kasia Muldner

IT Security vs. General IT

- Research question:
  - What differentiates security and general IT professionals?
- Motivation:
  - Current focus on general IT
  - Support tailored to security professionals (SP)

Differences Along Five Dimensions

Scope

Troubleshooting Complexity

Usability vs. Security Tradeoff

Fast-paced Environment

Perception by Stakeholders

Usability vs. Security

security professionals 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"

Perception and Environment

- Perception by stakeholders
  - Security professionals (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

Scope: Need for Broader Scope

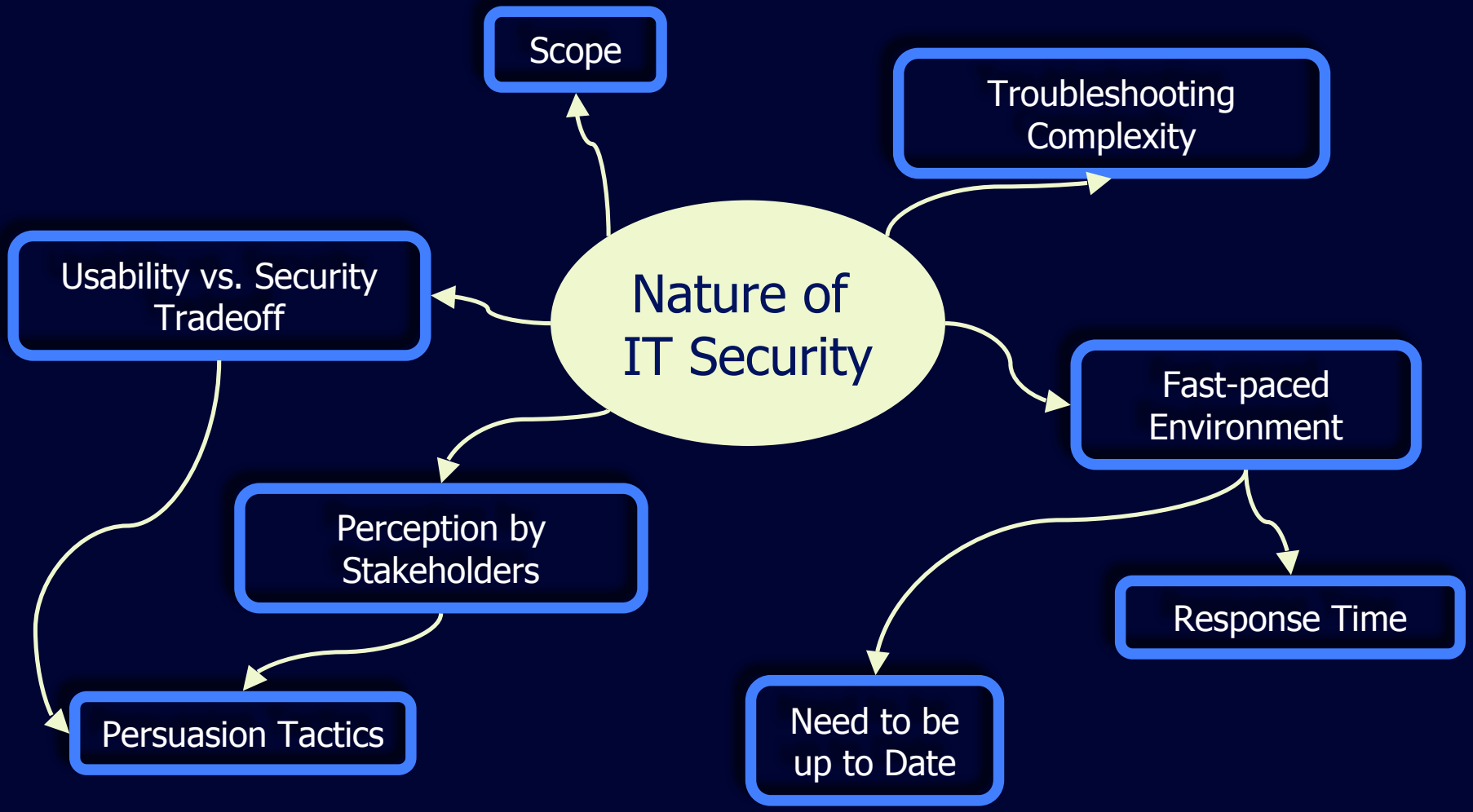
SPs need broader internal scope than general IT

"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"

SPs need broader external scope than general IT

Legislation (Patriot Act, Sarbanes Oxley)

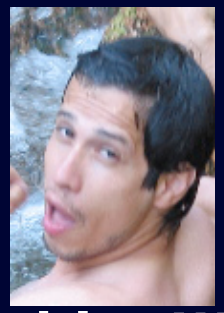
Model of Differences



A. Gagné, K. Muldner, K. Beznosov, "Identifying Security Professionals' Needs: a Qualitative Analysis", submitted to the *Symposium on Human Aspects in Information Security and Assurance* (HAISA) 2008.

Theme: Challenges

- Tasks & Tools
- IT Security vs. General IT
- Challenges
- Interactions
- Errors
- Management Model



Rodrigo Werlinger

Kirstie Hawkey

Theme: Challenges

- Research question
  - *What are the key challenges SPs face and how do the challenges interplay*?
- Motivation:
  - Related work has studied challenges *in isolation*

Challenges: Technological

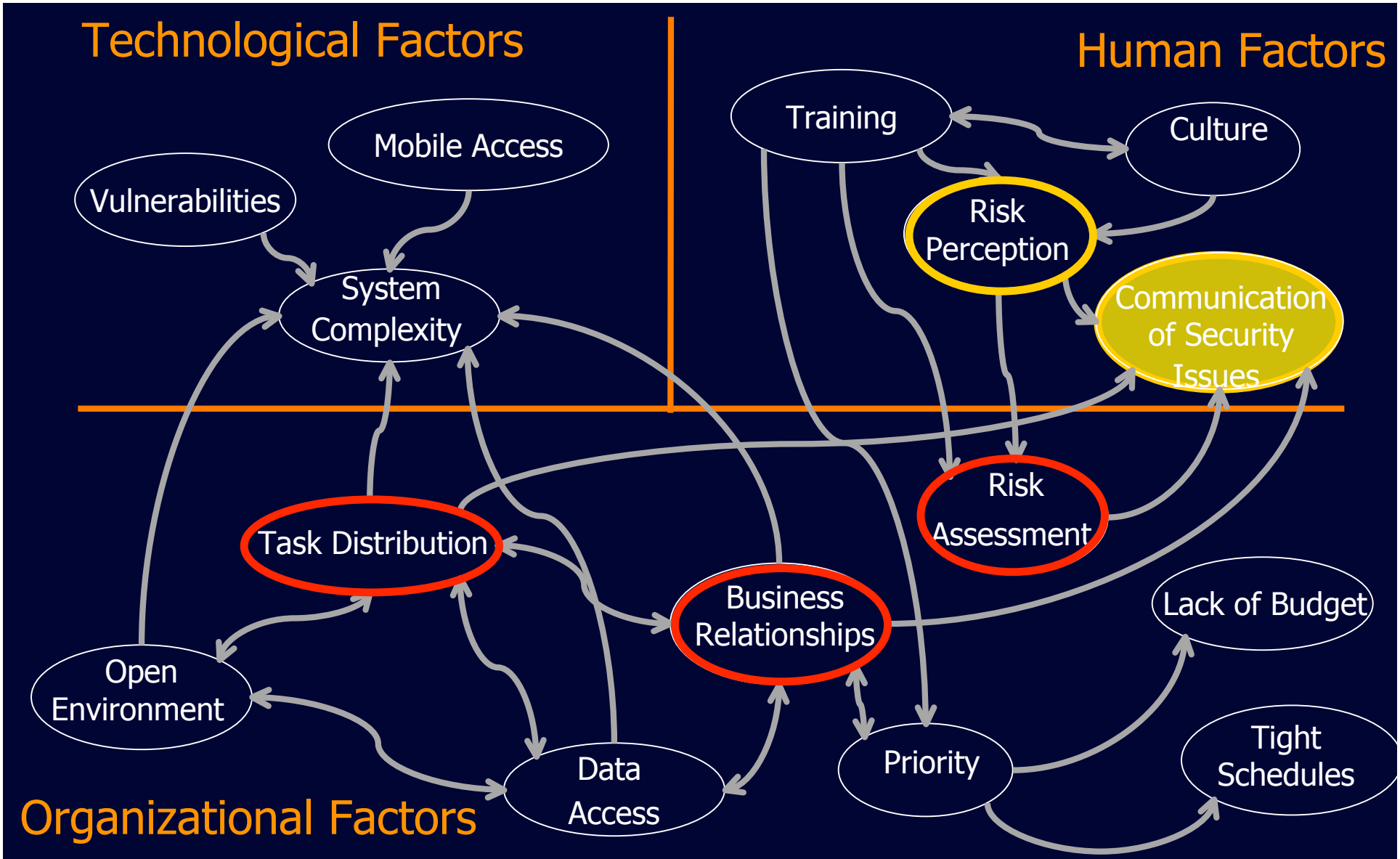
- Vulnerabilities
- System Complexity
  - A typical network could have firewalls, DMZs, proxies, switches behind the firewall, routers in front of the firewalls, mail servers and not enough people to look after the overall security of these interconnected devices
- Mobile Access
  - Mobile user access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

Challenges: Human

- 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

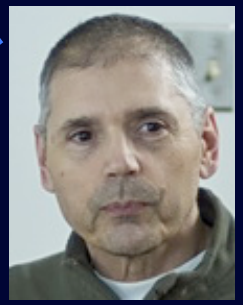
Risk Assessment	Difficult to estimate IT security risks
Business Relationships	Misaligned security policies make it challenging to enforce standards within an organization
Security Low Priority	Security is not a priority for many stakeholders
Task Distribution	Distribution of responsibilities was an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



R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", submitted to *HAISA '08*.

Theme: IT Security vs. General IT

- Tasks & Tools
- IT Security vs. General IT
- Challenges
- Interactions
- Errors
- Management Model



David Botta

Kasia Muldner

Theme: Errors

- Research Question:
  - *What leads to errors in security processes?*
- Motivation:
  - Breakdowns during IT security management can put organizations at risk
  - Need for understanding the causes

Terminology

- Error:

  "*a failure of a structure or process is an indication of error only to the extent that it prevents maximizing the outcomes of interest to the patient*"
  [Hofer]

- IT security:
  - the patient = organization
  - Error = occurrence when security practices that do not maximize outcomes of interest, i.e., *sub-optimal situations*

Suboptimal Situations

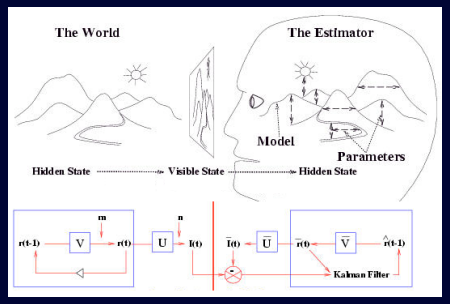
- Distributed and complex nature of IT security management

Suboptimal situations, i.e., errors

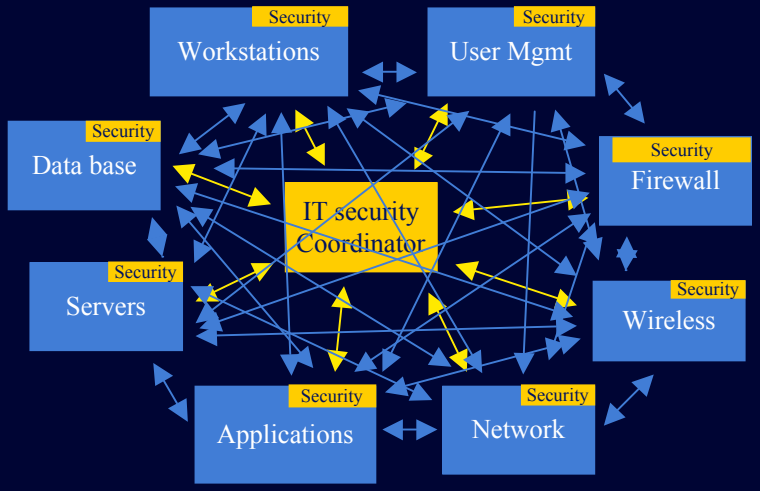
- Busby's framework for errors in a distributed system that includes:
  - Cues: an occurrence which ``*participants use to determine when to act and how to act*''
  - Norms: rules of some sort that help make the participants' subtasks consistent with each other
  - Transactive memory: is a type of mutual understanding, in which people in a group mutually know who is responsible for what
- Errors arise as a result of breakdowns in mutual understanding, cues, norms and transactive memory

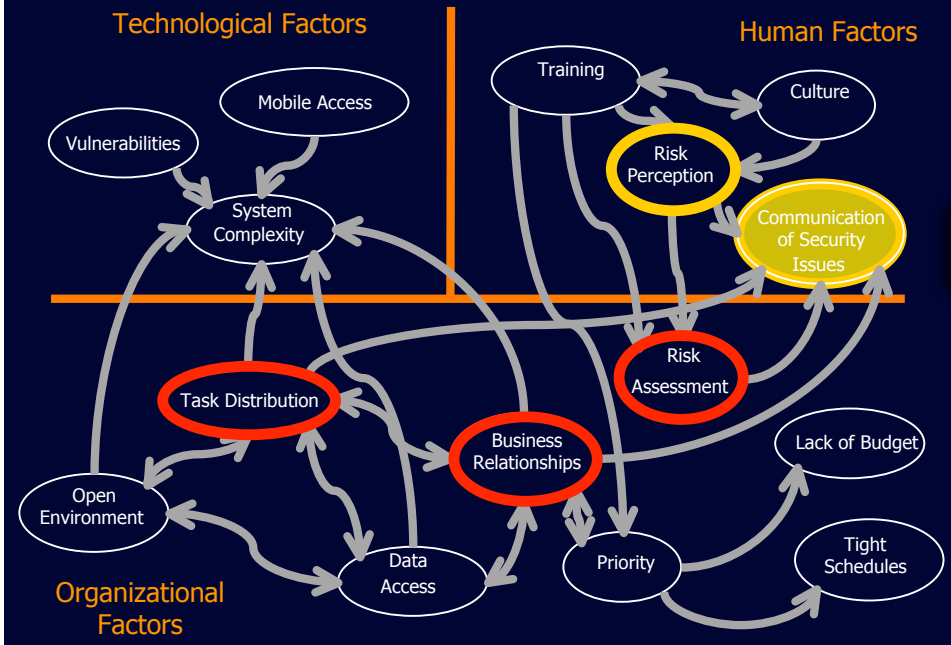
Summary

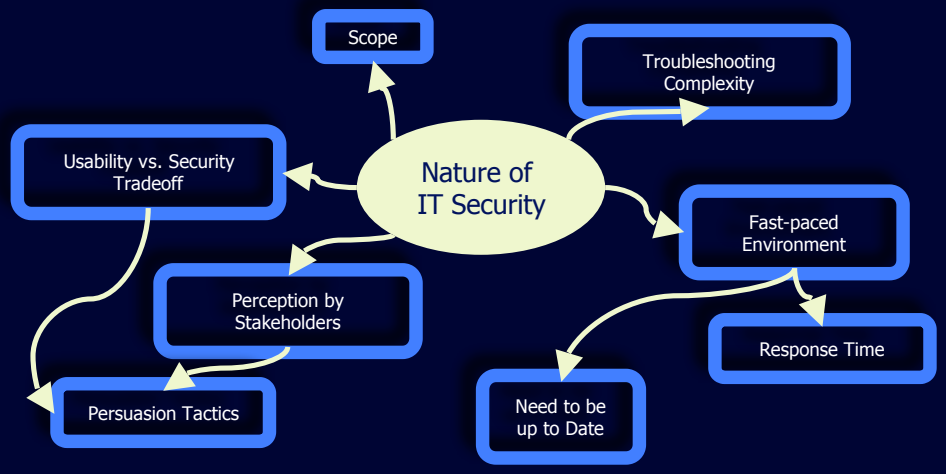
Field study



Models







Putting It All Together

- Complexity of IT security management
- Understanding of IT security professionals
- Guidelines for tool refinements and directions for future research

Future Challenges

- Creating testable models for validating and extend findings?
- Transforming guidelines into concrete tool refinements?
- Evaluating tools refinements given the complex and distributed nature of IT security?

hotadmin.org

lersse.ece.ubc.ca