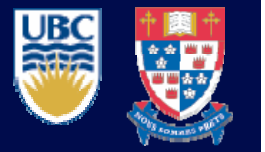


Towards Understanding IT Security Professionals and Their Tools

David Botta, Rodrigo Werlinger, André Gagné
Konstantin Beznosov, Lee Iverson, Sidney Fels
University of British Columbia

Brian Fisher
Simon Fraser University

IT Security is Critical

IT Security is Expensive

organizations worldwide to spend 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

How to Develop Better Tools?

- How tools are actually used?
- What works & what doesn't?
- What needs to be improved?

Outline

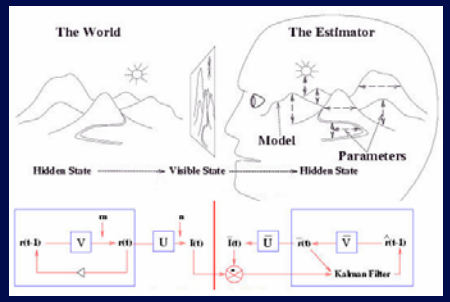
- HOT Admin project
- How We Did the Study
- What we got
- Summary

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

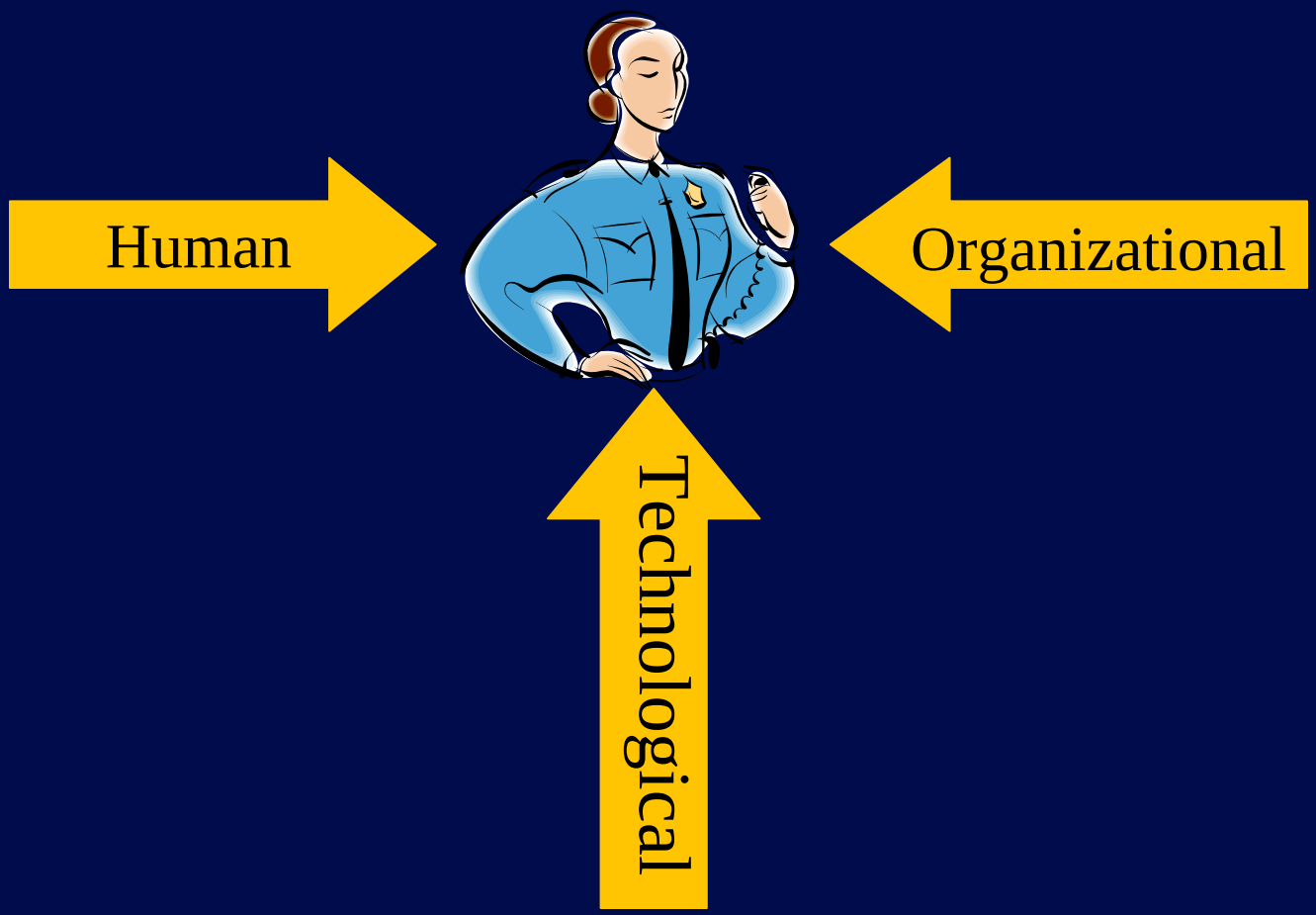
sponsors and partners

Entrust

NSERC CRSNG

SAP

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

Simplify & Centralize Win
Management tasks are centralized and made simple. Great Admin Tool!
www.softwareshelfdistribution.com

Hot Babes In Your Bed
Loneliness Sucks - Fill Your Life With Hot Babes. Video Example!
www.PickUp101.com

Filipinas look for love
Pretty girls from Philippines look for serious relation worldwide
www.filipinokisses.com

Sexy Russian Babe
Find a Hot Russian Babe Online E-mail Amazing Girls Today!
www.Anastasiaweb.com

Third Party Verification
Automated or Live Agent Turn-key, No Capital Costs
www.intelemedia.com

Red Hot Deals
Update your fall look for less with sweet deals on sexy red boots
www.personalshopper.com

Sizing Guide for MySQL
Free Sizing Guide and Performance Benchmarks for MySQL on Blade
www.mysql.com

Sexy women, jt tinney
jt tinney bikini girls stacey hayes Playboy Model Louise Glover, babes
www.knockoutmag.com

Related Categories

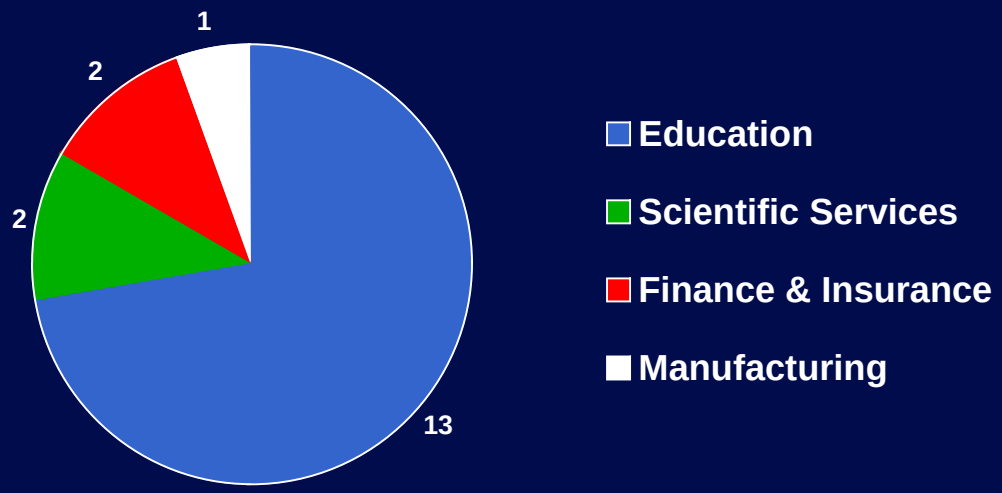
- Hot Blonde
- Hot Bra
- Hot Celebrities
- Hot Clothing
- Hot Ladies
- Hot Legs
- Hot Swimsuit
- Hot Wallpapers
- Hot Asian
- Hot Cup

How We Do the Study

Data Collection

Questionnaires: 28

Interviews: 18



Analysis

Focus Topics → Themes → Theory Building

- Activities
  - Prioritization
  - Skills
  - Knowledge
  - Resources
- Tools
  - What
  - Why
  - How
- Errors
  - Prevention
  - Detection
  - Recovery
- Communication
  - Common ground
  - Coordination
  - Decision making

- Activities
- Tools
- Usability issues

Grounded Theory

What We Got

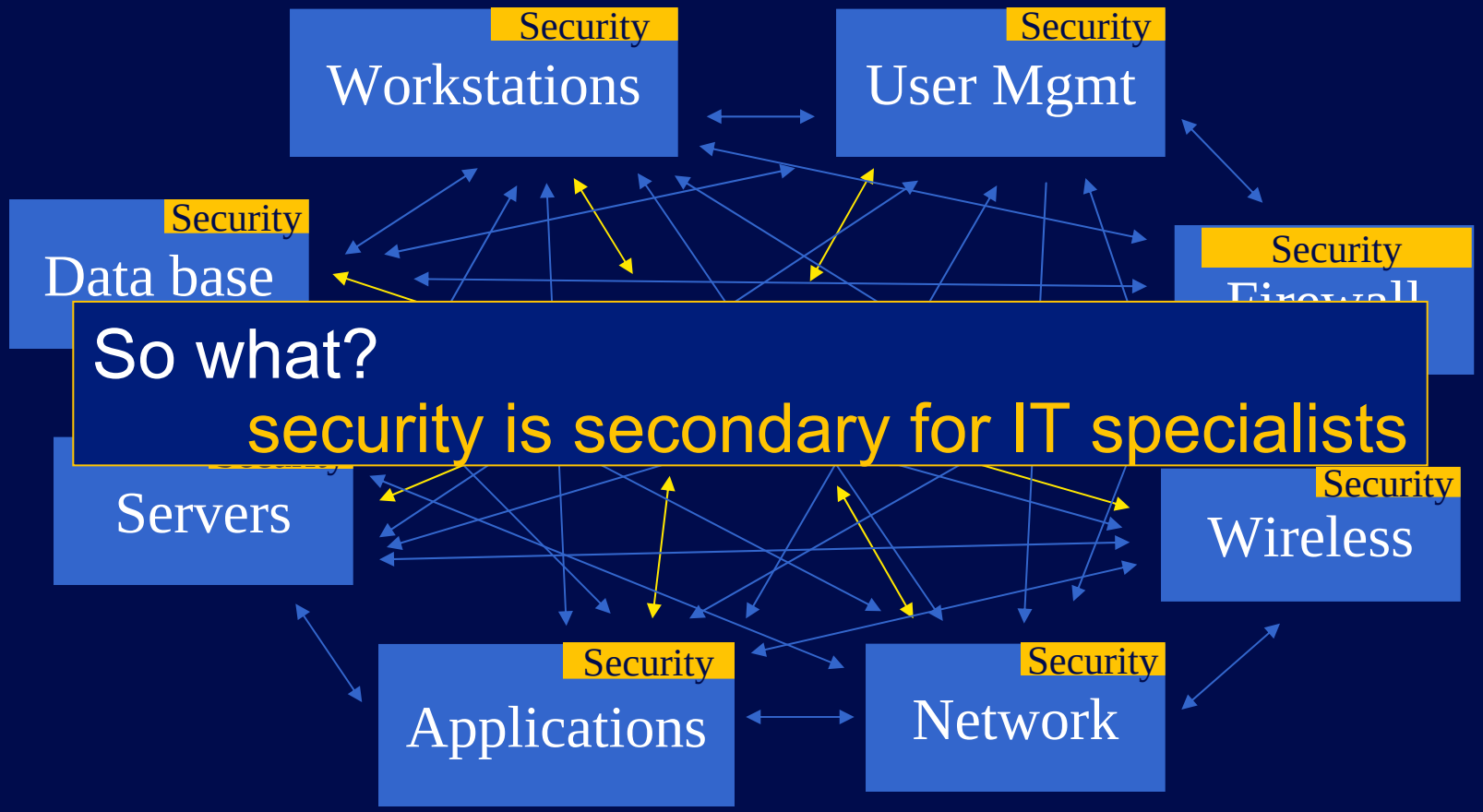
No Security Admins!

- 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/tools

Activity Chain

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

So what?

- Dependence
- Short term decision making
- Deployment of
  - Resources
  - Knowledge
  - Skill

Skills: Tacit Knowledge and Creativity

- Pattern recognition & inferential analysis
- *Bricolage*
  - The construction or creation of a work from a diverse range of things which happen to be available

So what?

- Finding gaps in support
- New kinds of tools
- Tool improvement
- New usability testing methods

They Wanted Tools That:

- Can be accessed from office, home, hotel
- Can fit with existing management practices
  - customizable
  - flexible reporting
- Offer ease of practical documentation
- Minimize the risk of overlooking critical information
- Minimize workload

Summary of IT Security Management Characteristics

- Loosely coordinated teams
- Security distributed over different kinds of responsibility
- High level of tacit knowledge and creativity

hotadmin.org

lersse.ece.ubc.ca