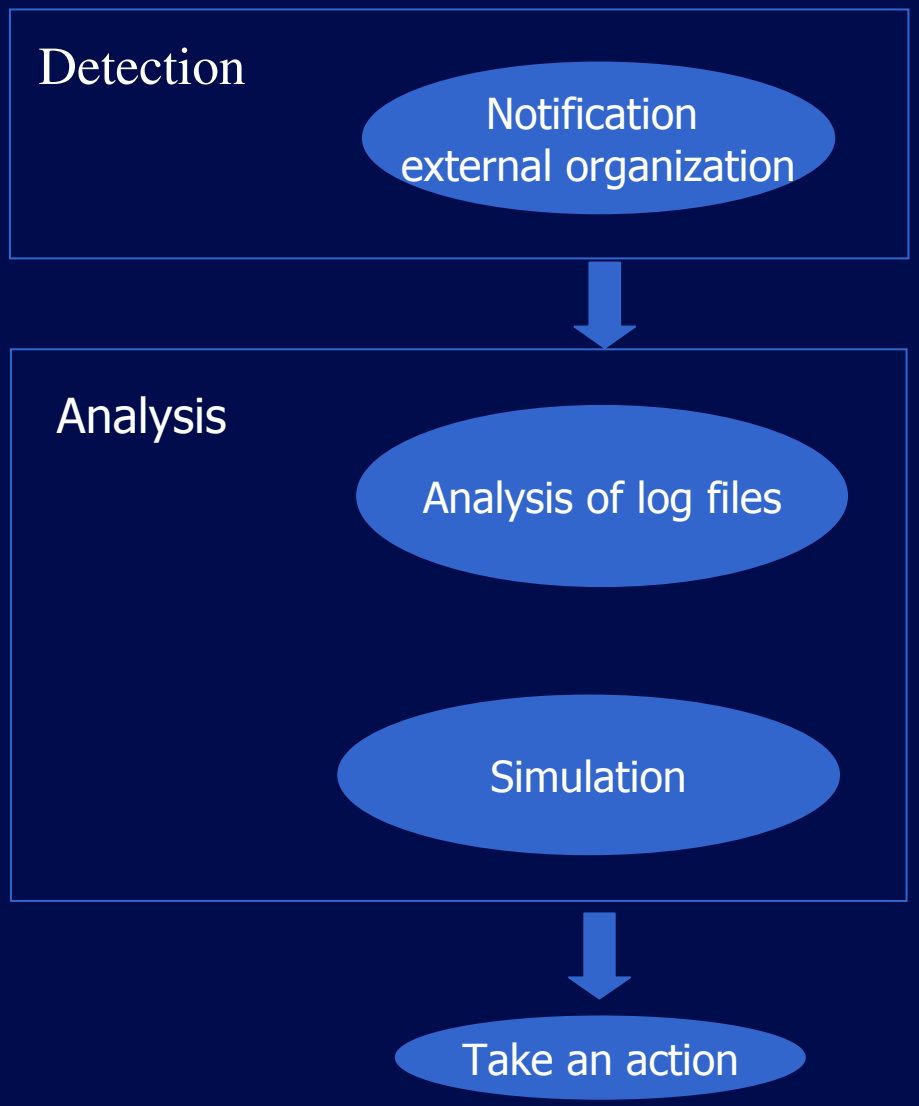
Responding to security incidents: are security tools everything you need?

Rodrigo Werlinger, Kirstie Hawkey, Konstantin Beznosov
University of British Columbia, Vancouver, Canada

Malicious software flooding the network



Resources:
Specially security tools
- *TCPDump*
- *Ethereal*
- *Antivirus*

+ Some skills
- *Pattern recognition*
- *Hypothesis generation*

A client sending SPAM

Resources

- Almost no security tools!

- Intensive collaborations

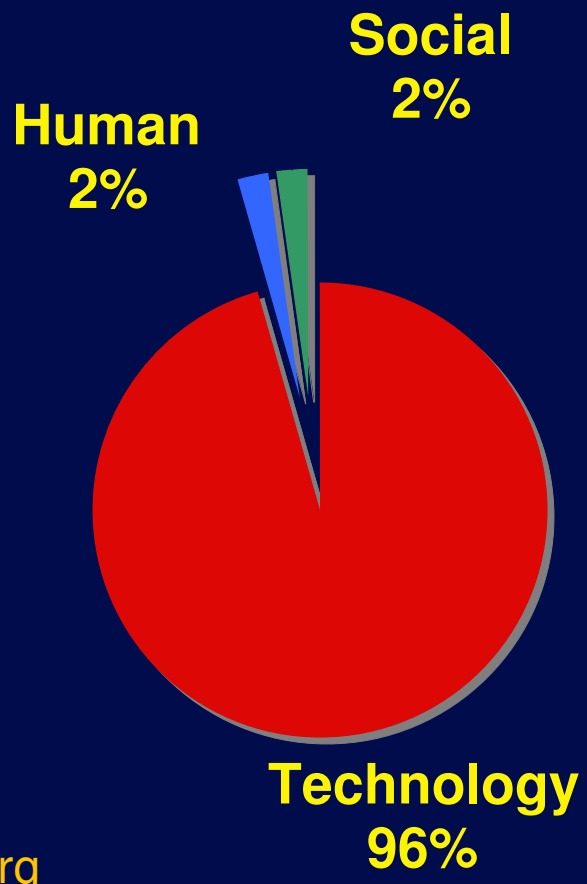
- Tacit knowledge

- Need for new procedures

…A lesson from 1988 that has not been learned is that communication is critical in addressing the problem…

Eugene Spafford, 2003

Emphasis on technical issues



engineeringvillage2.org
Compendex -- 9M engineering references and abstracts
Inspec -- 8M records from scientific and technical journals and conferences

Konstantine Beznosov, HAISA 2007

Technical presentations FIRST 2007

- Main talks: 26 technical from 42 ~ 62%
- Tutorials: 4 technical from 5 ~ 80%
- Best practices: 14 technical from 16 ~ 88%

What other aspects are important?

What we wanted to know

- Human, organizational, and technical challenges for security practitioners
- Resources (not only tools) security practitioners use to respond to incidents
- Potential breakdowns with security standards

Outline

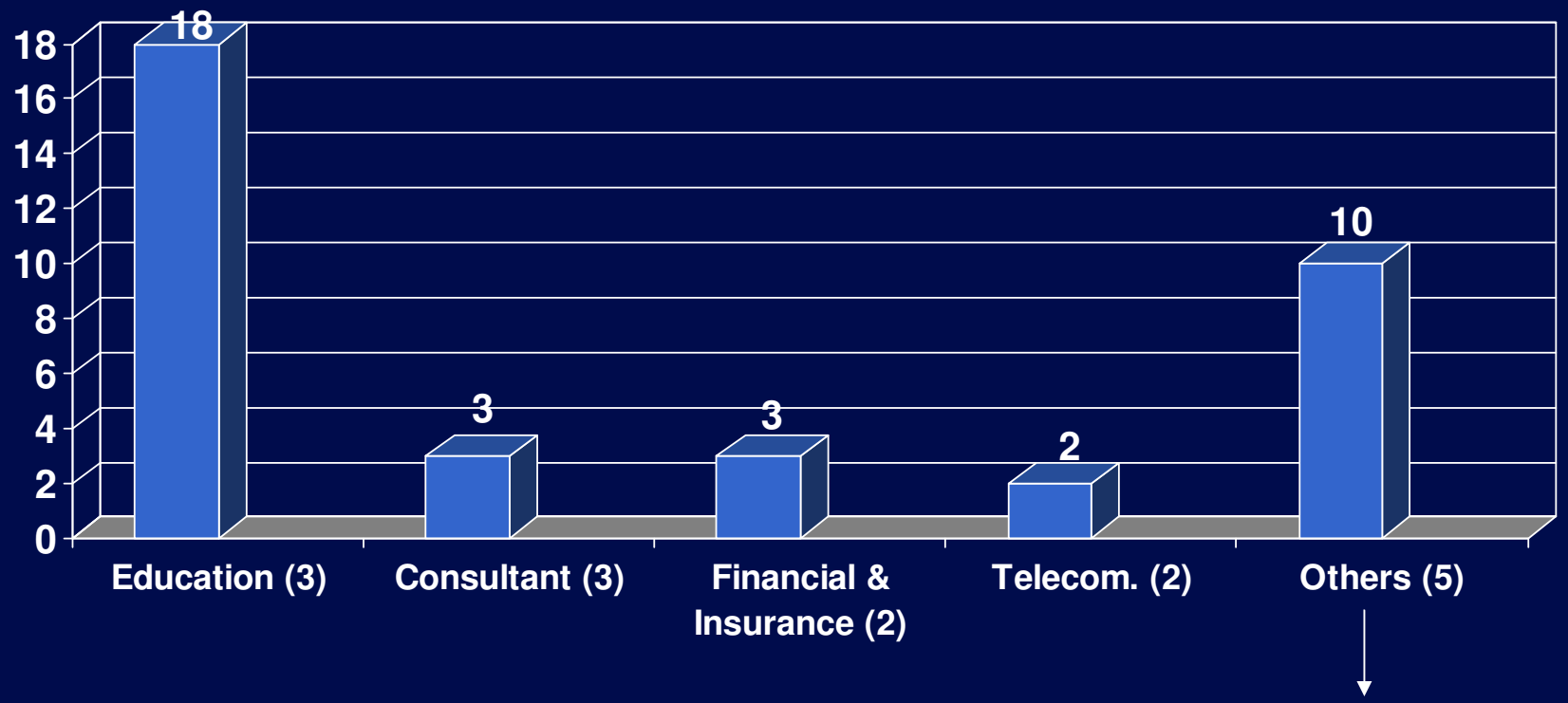
- Motivation and context
- Approach
- Results & Discussion
  - The setting: challenges
  - Incidents described
  - Resources used
- Lessons learnt
- Wrap-up

Empirical data

- Semi-structured Interviews
- Participatory observation
- Qualitative analysis:
  - Find patterns/relationships in the data

Our sample

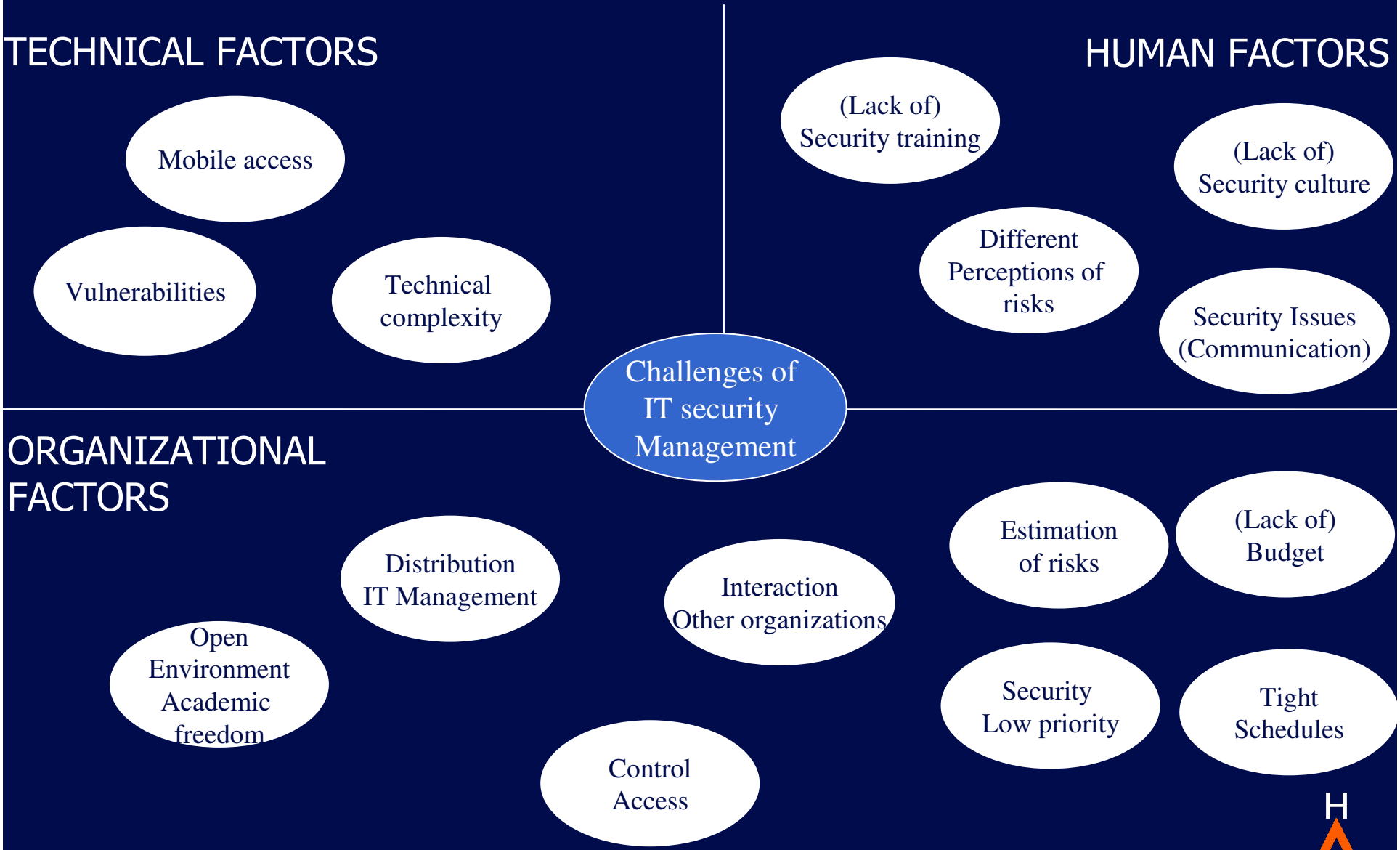
Semi-structured interviews: 34
Participants: 36
Number of organizations: 17



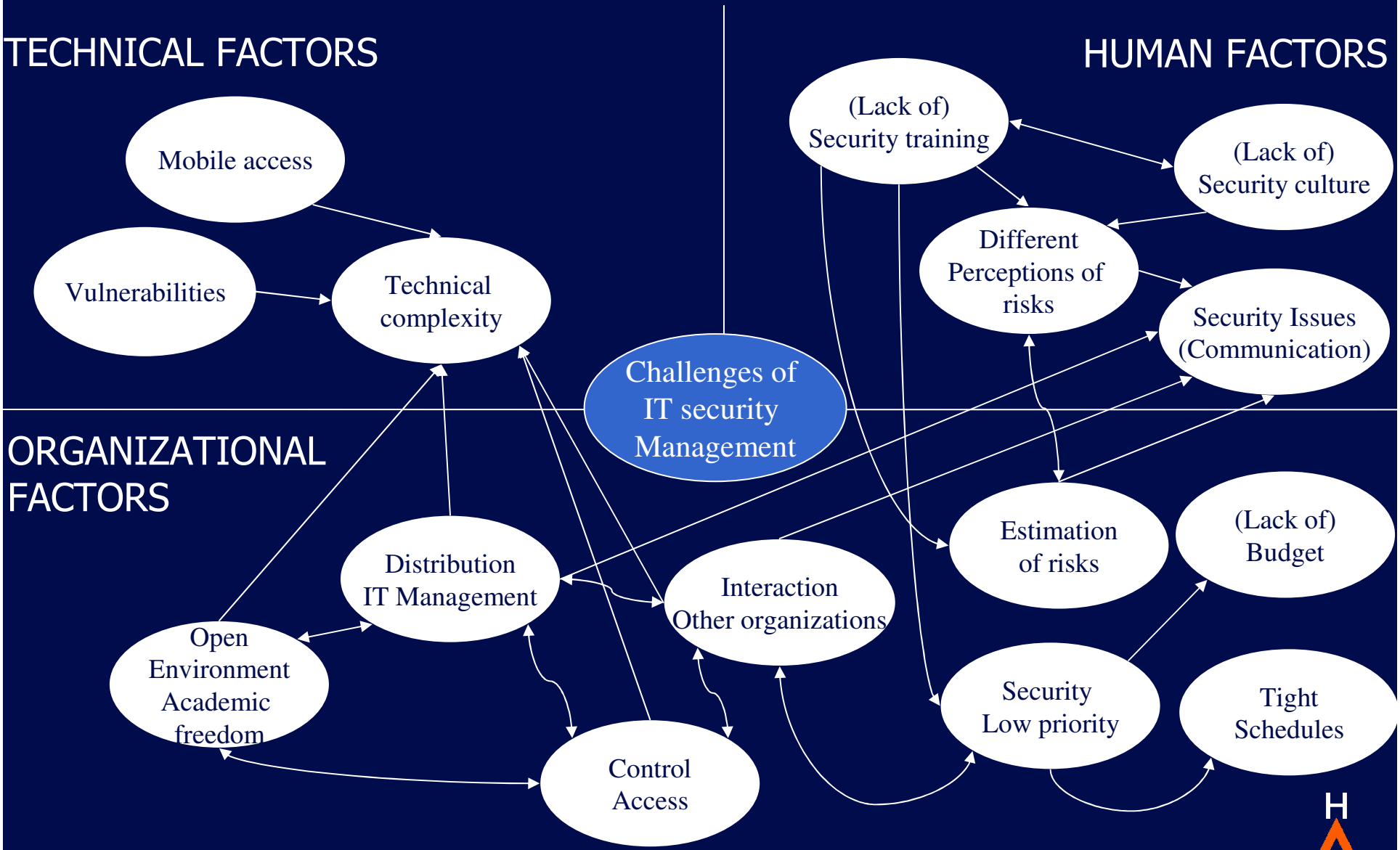
Outline

- Motivation and context
- Approach
- Results & Discussion
  - The setting: challenges
  - Incidents described
  - Resources used
- Lessons learnt
- Wrap-up

Security challenges



Interplay of Security challenges



Consider the whole picture

Security in organizations is characterized not only by :

- Size
- Sector
- Top Management Support
- External factors (e.g., Customer requirements)

Kankanhalli, et al. (2003)

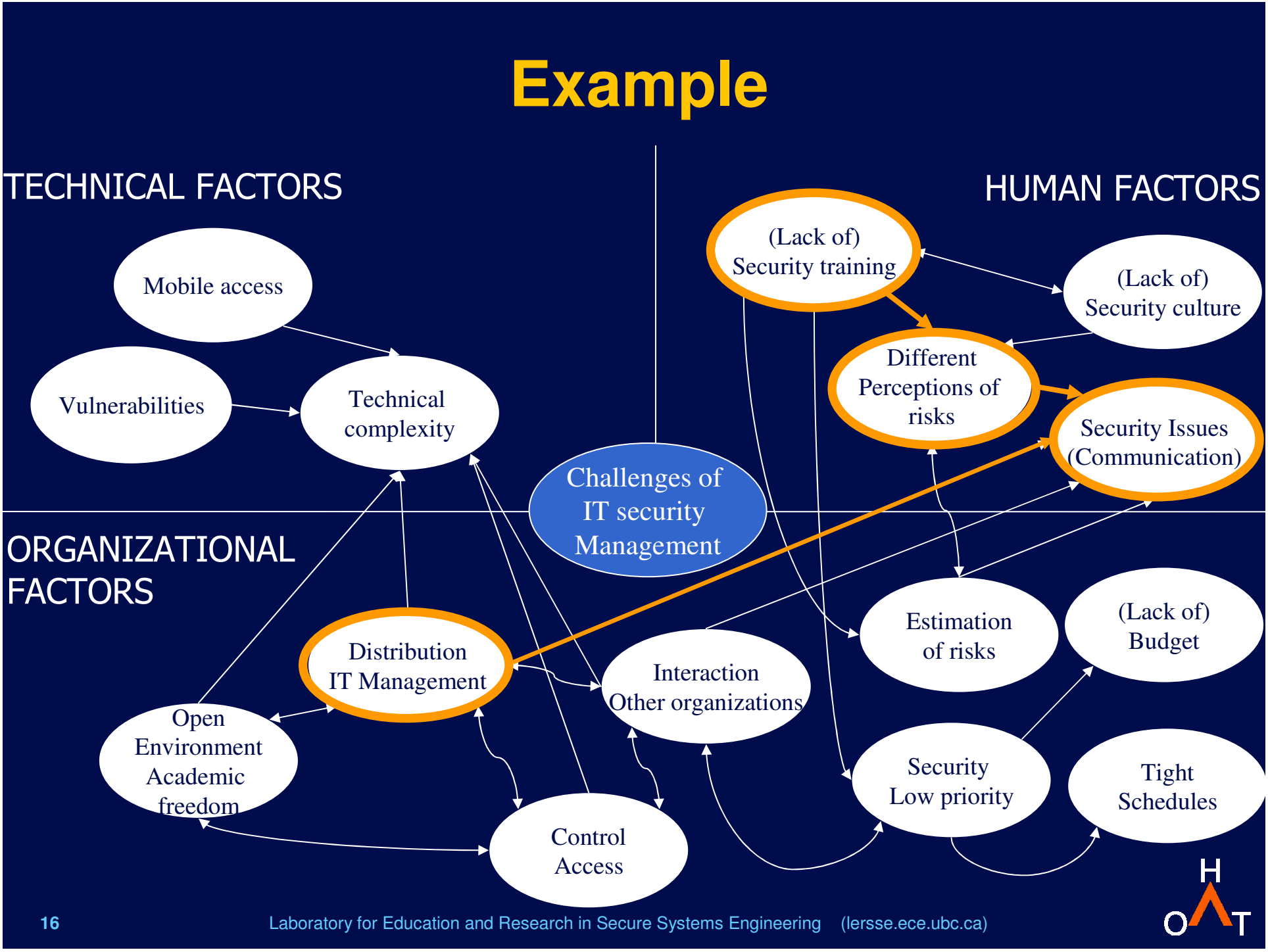
Chang & Ho (2006)

But also by:

- Security Challenges, Werlinger et al., (2008a)

All this factors affect security decisions within organizations (e.g., purchase new security tools, response to security incidents

Example


TECHNICAL FACTORS
HUMAN FACTORS
ORGANIZATIONAL FACTORS
Mobile access
Vulnerabilities
Technical complexity
(Lack of) Security training
(Lack of) Security culture
Different Perceptions of risks
Security Issues (Communication)
Challenges of IT security Management
Distribution IT Management
Interaction Other organizations
Estimation of risks
(Lack of) Budget
Open Environment Academic freedom
Control Access
Security Low priority
Tight Schedules

Mentioned incidents

- Malicious SW = 8 instances
  - Hosts
  - End-users' PCs
  - Large outbreaks
- Spam, Phishing = 3 instances
- Suspected incidents = 7 instances
  - Network slow
  - Port scanning

Tasks, skills, tools

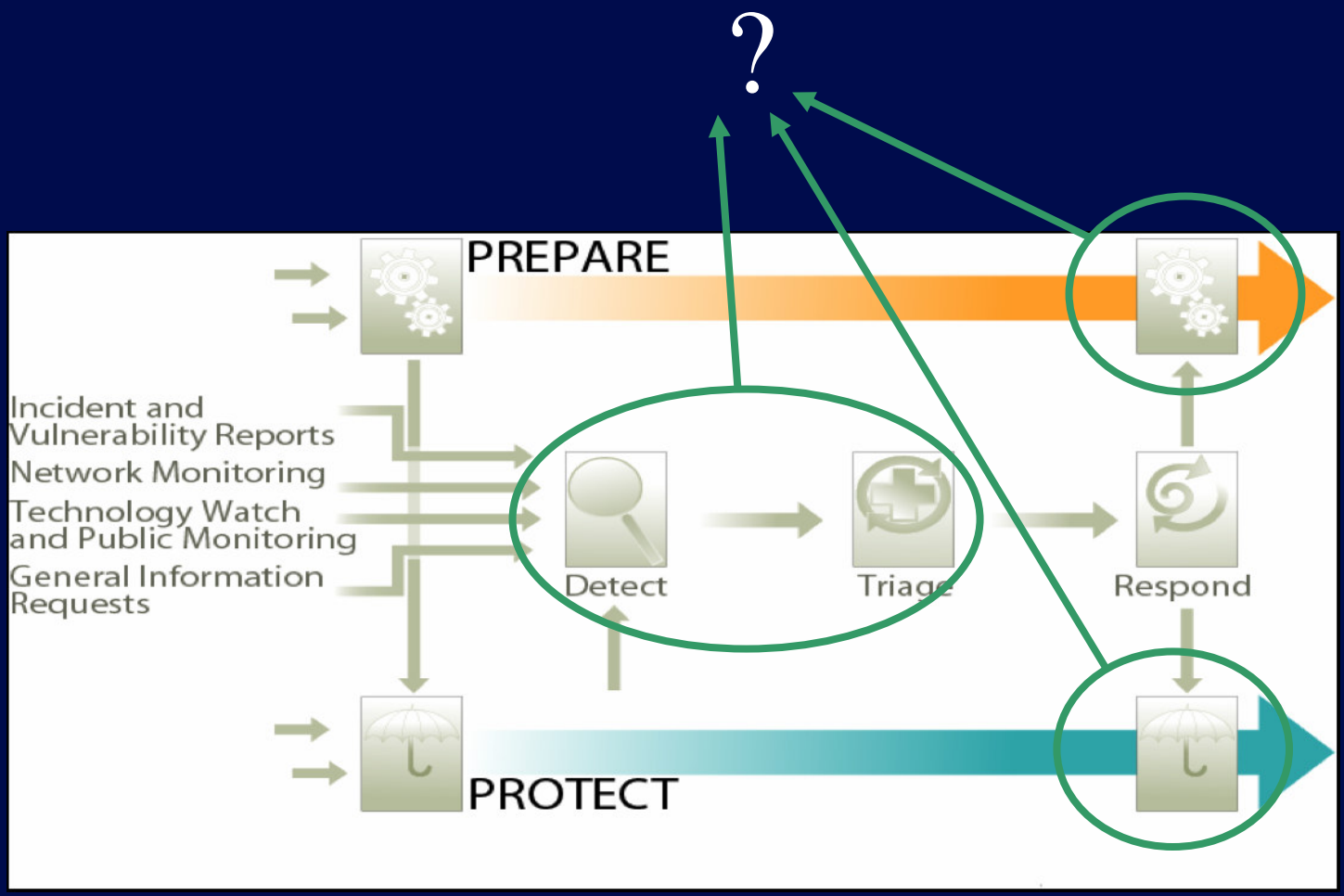
Detection

- Monitoring
- Receiving notifications
- Pattern recognition
- Communication
- Scripts, IDS
- Incident ticketing system

Analysis

- Verification
- Assessing
- Tracking down the source of the anomaly
- Hypothesis generation
- Pattern recognition
- Communication
- Scripts, IT administration tools
- Antivirus

Potential breakdowns with standards



Incident Management Georgia Killcrece, Software Engineering Institute,

Lessons

- Need for more "human-organizational" training
- Need for developing standards to exchange security information
- Improve security tools:
  - Integration of communication channels
  - Collaboration features
  - Flexible reporting capabilities

Wrap-up

- Two different examples of security incidents
- Need for considering human-organizational aspects
- List of tasks, skills and tools
- Possible breakdowns with standards
- Lessons

What's next

- More data to validate our findings
- Develop scenarios/standards/procedures
  - Training
  - Communicate with other organizations
  - Communicate internally
- More support from tools
  - Integrate communication channels
  - Better reporting

Thank you

rodrigow@ece.ubc.ca