A Broad Empirical Study 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 Expensive

IT Security is Expensive

organizations worldwide spent in 2007

$1.55 trillion on IT

7-9% on IT security

IT Security is Expensive

organizations worldwide spent in 2007

$1.55 trillion on IT

7-9% on IT security

$108 billion

IT Security is Expensive

organizations worldwide spent in 2007

$1.55 trillion on IT

7-9% on IT security

$108 billion

Forrester Research

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

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

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 **O**rganization and **T**echnology Centred Improvement of IT Security **Admin**istration

sponsors and partners

Entrust

NSERC CRSNG

SAP

HOT Admin:
Human **O**rganization and **T**echnology Centred Improvement of IT Security **Admin**istration

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

sponsors and partners

Entrust

NSERC CRSNG

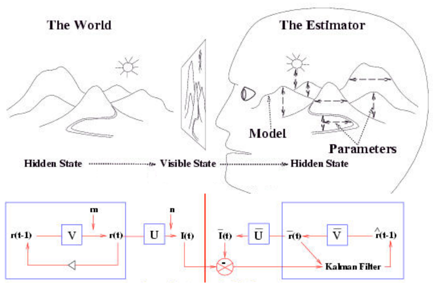
SAP

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

sponsors and partners

Entrust

NSERC CRSNG

SAP

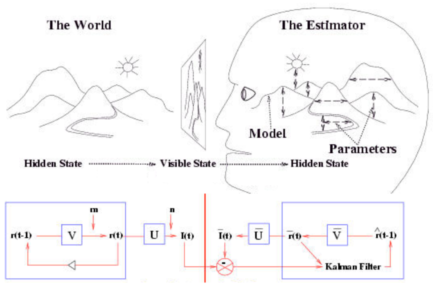
HOT Admin:
Human **O**rganization and **T**echnology Centred Improvement of IT Security **Admin**istration

H O T

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

Work Plan

Field study



Models

Techniques & Methodologies

sponsors and partners

Entrust

NSERC CRSNG

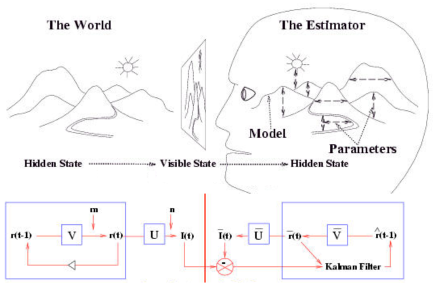
SAP

HOT Admin:
Human **O**rganization and **T**echnology Centred Improvement of IT Security **Admin**istration

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

Work Plan

Field study



Models

Techniques & Methodologies

Validation & Evaluation

sponsors and partners

Entrust

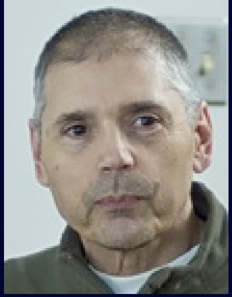
NSERC CRSNG

SAP

Project Team

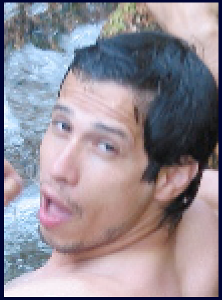
Dr. Konstantin Beznosov

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



Dr. Sidney Fels

- Assoc. Prof., ECE, UBC
- new interfaces design



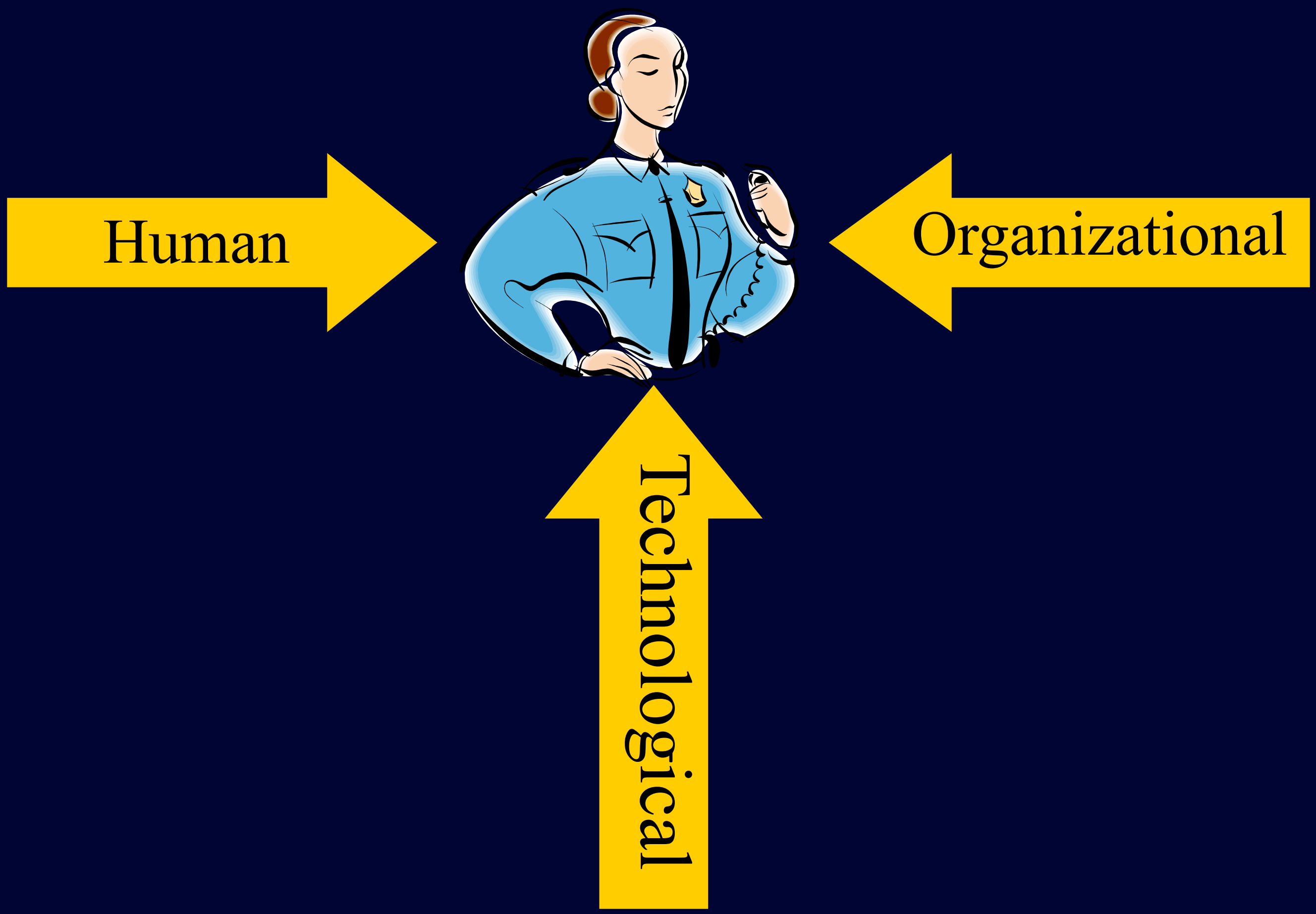
Dr. Brian Fisher

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

Dr. Lee Iverson

- Assist. Prof., ECE, UBC
- Inform. visualiz.
- collaboration infrastructures

Human Organization and Technology Centred

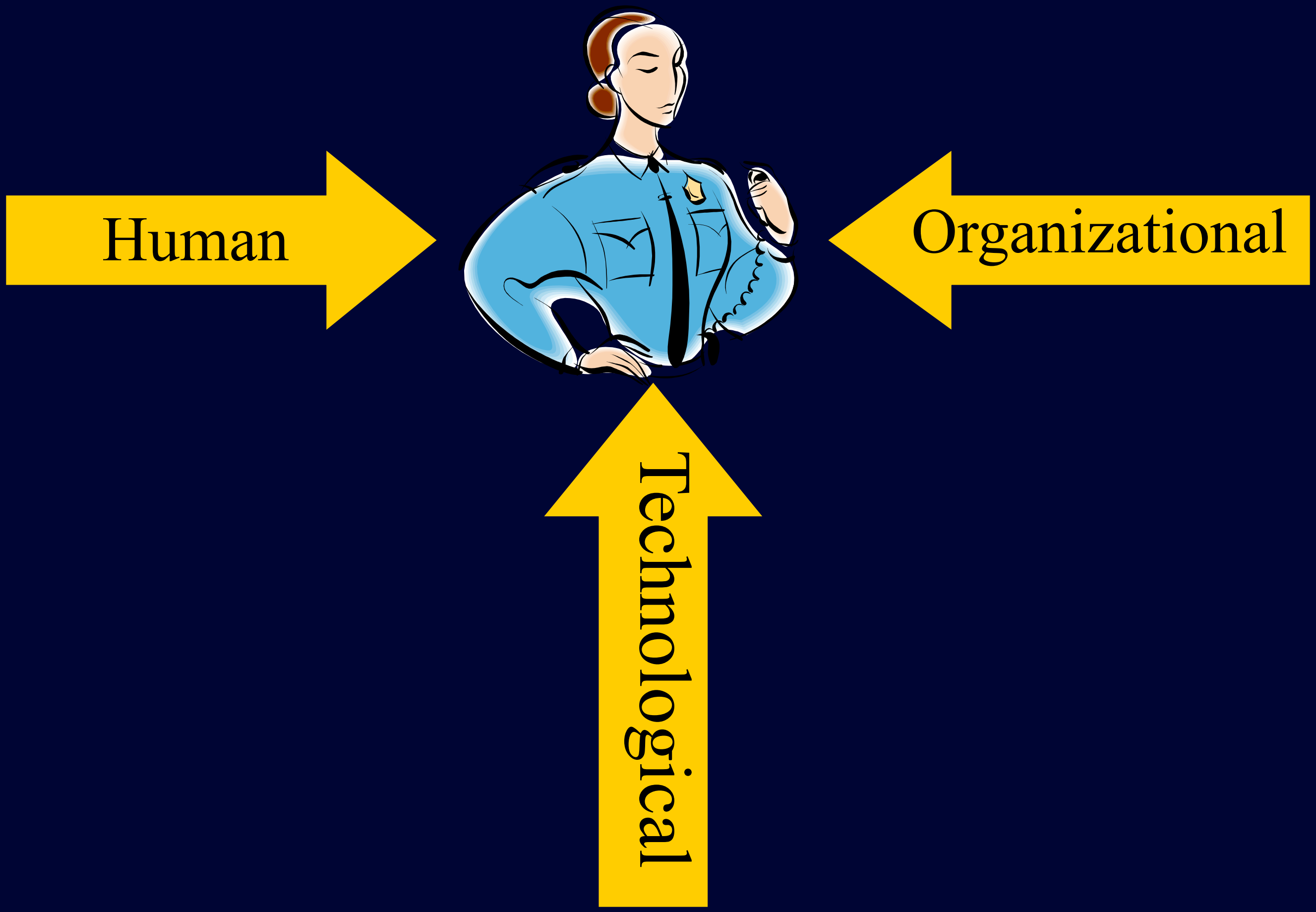


Human

Organizational

Technological

Human Organization and Technology Centred

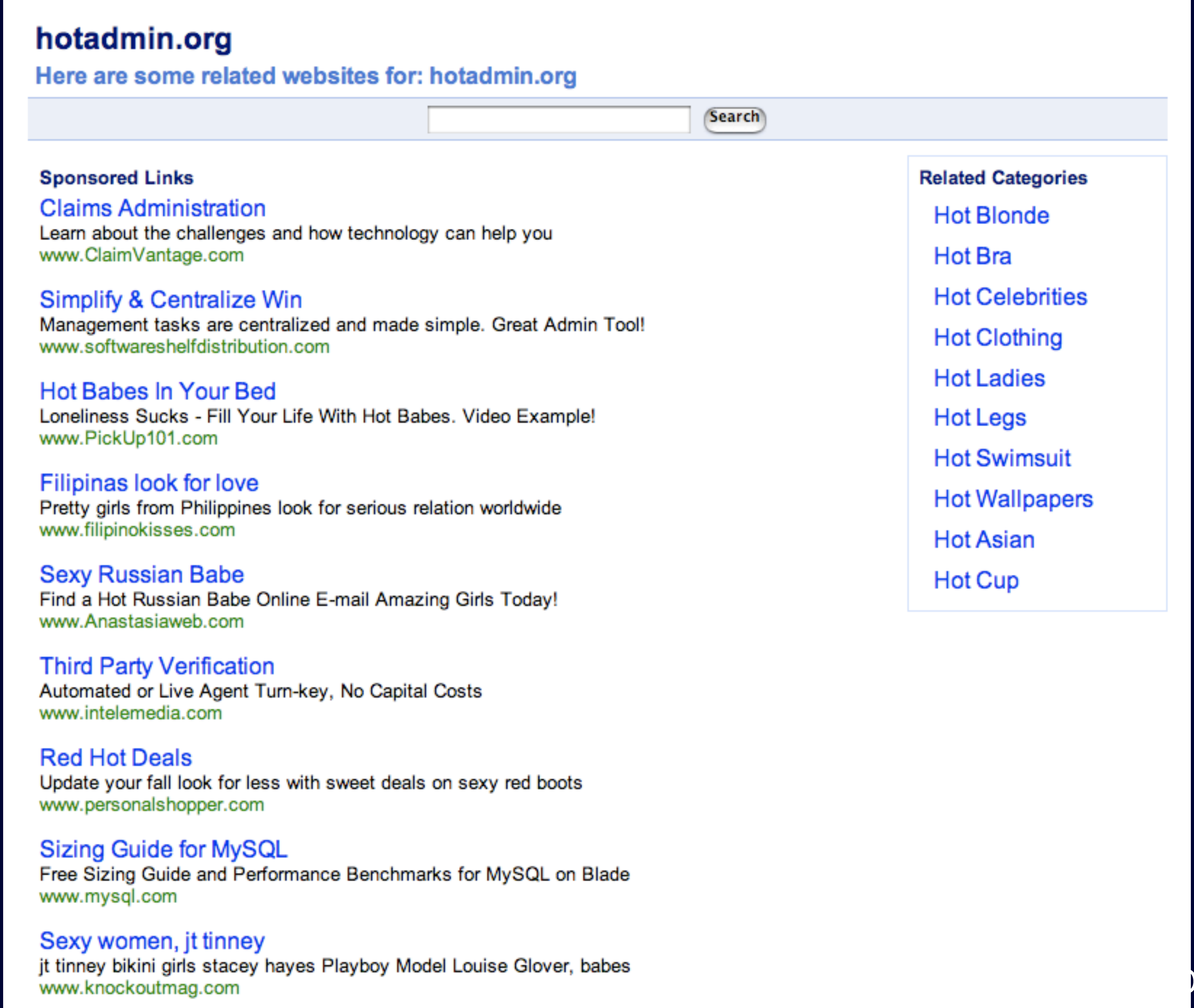


Human

Organizational

Technological

hotadmin.org



hotadmin.org

Here are some related websites for: hotadmin.org

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

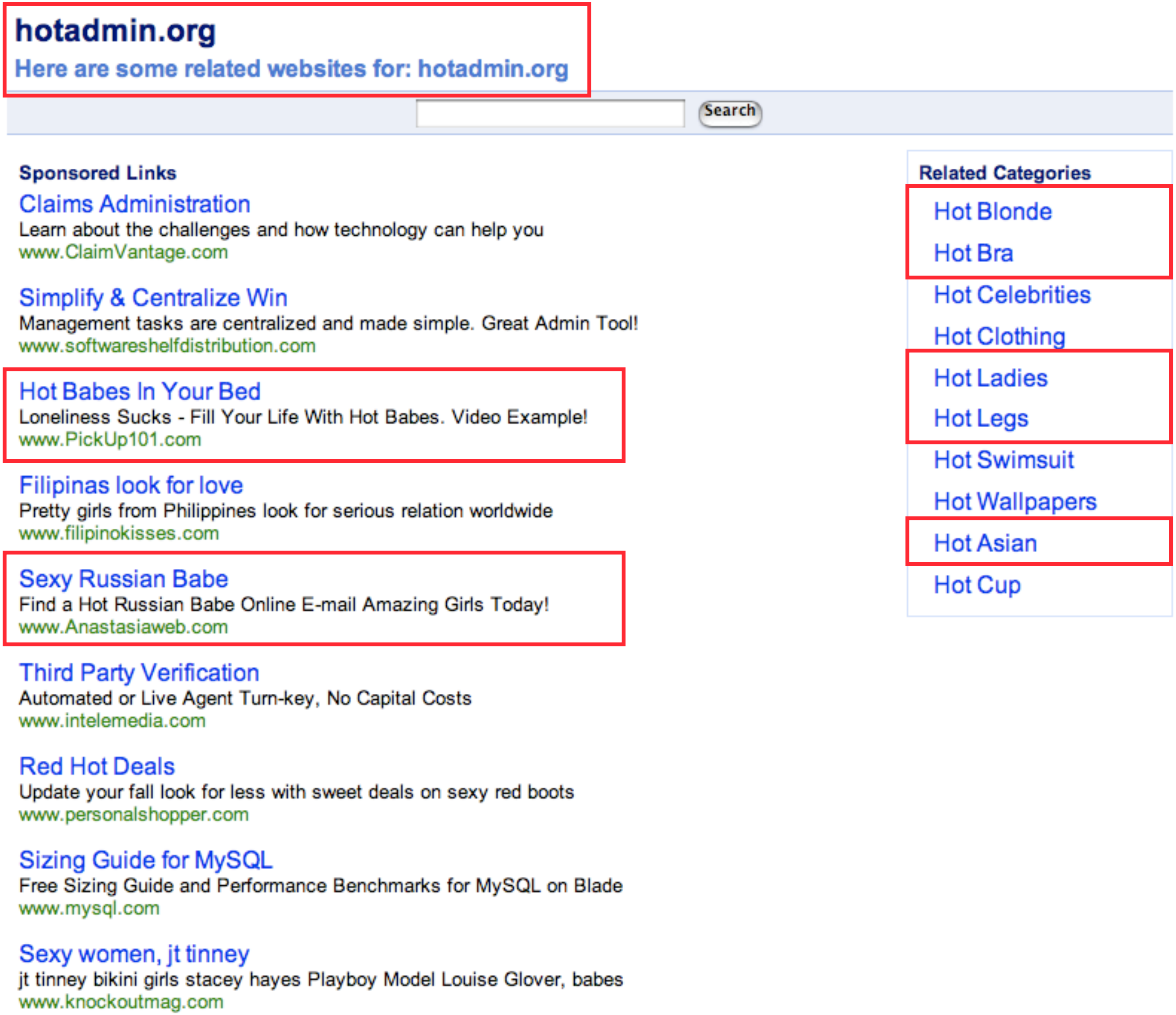
Red Hot Deals
Update your fall look for less with sweet deals on sexy red boots
www.personalshopper.com

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



hotadmin.org

Here are some related websites for: hotadmin.org

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

Methods

Recruitment

Recruitment

Challenges

- Overworked
- Secrecy culture
- Backstage

Recruitment

Challenges

- Overworked
- Secrecy culture
- Backstage

Approaches

- Professional contacts
- Practical benefits
- Gradual recruitment
- Gatekeepers

Recruitment

Challenges

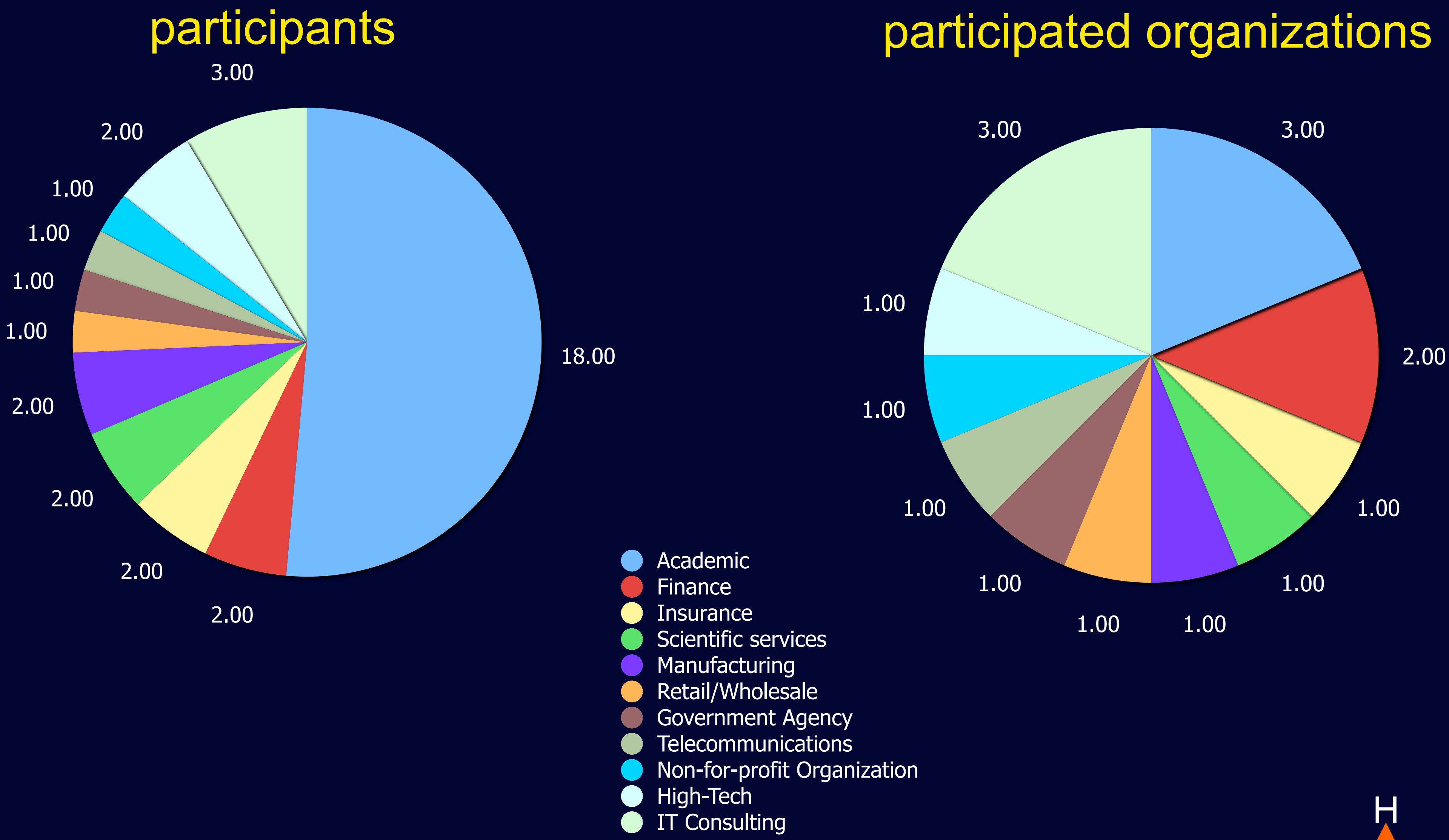
- Overworked
- Secrecy culture
- Backstage

Approaches

- Professional contacts
- Practical benefits
- Gradual recruitment
- Gatekeepers

As of March 2008, 34 interviews with 36 participants

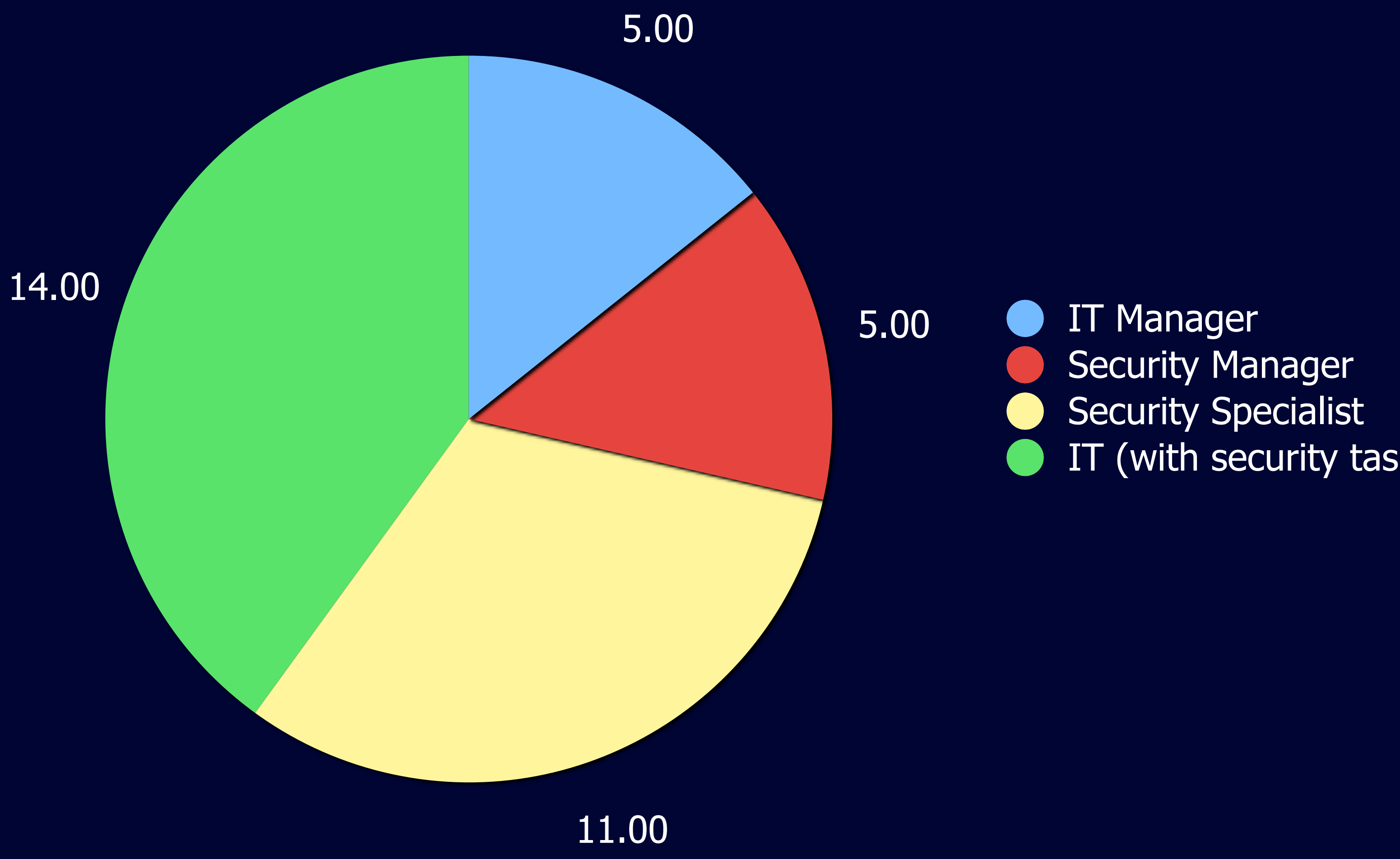
Industry Sectors



participants

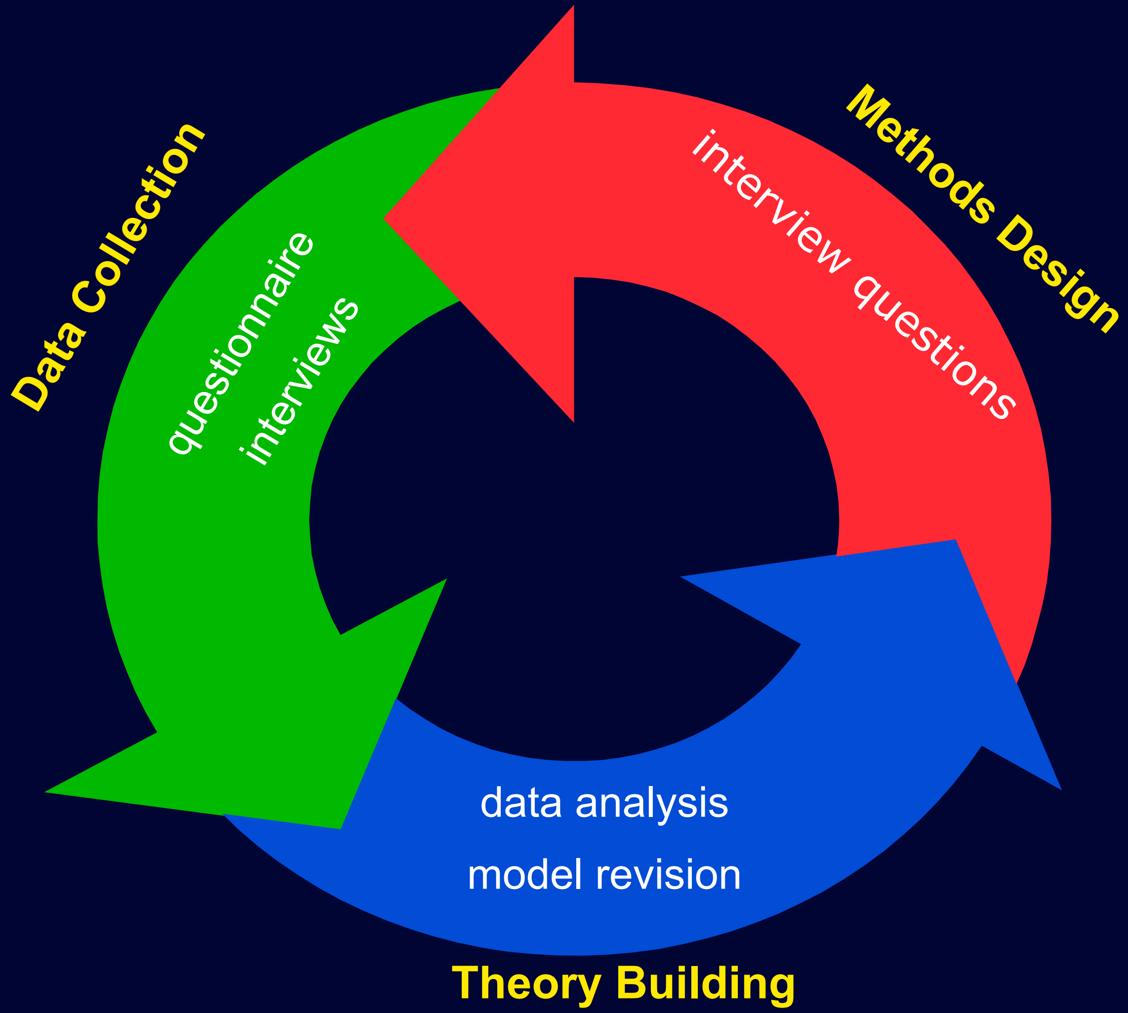
participated organizations

Job Types


5.00
5.00
11.00
14.00
IT Manager
Security Manager
Security Specialist
IT (with security tas

Analysis

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

Theme: Tasks and Tools

Tasks & Tools

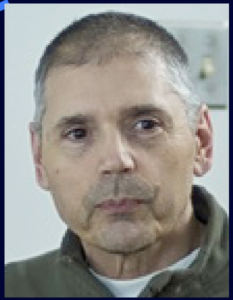
IT Security vs. General IT

Challenges

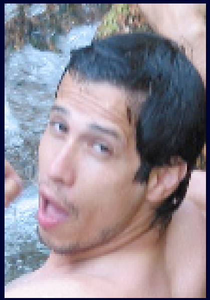
Interactions

Errors

Management Model



David Botta



Rodrigo Werlinger

André Gagné

No Security Admins!

No Security Admins!

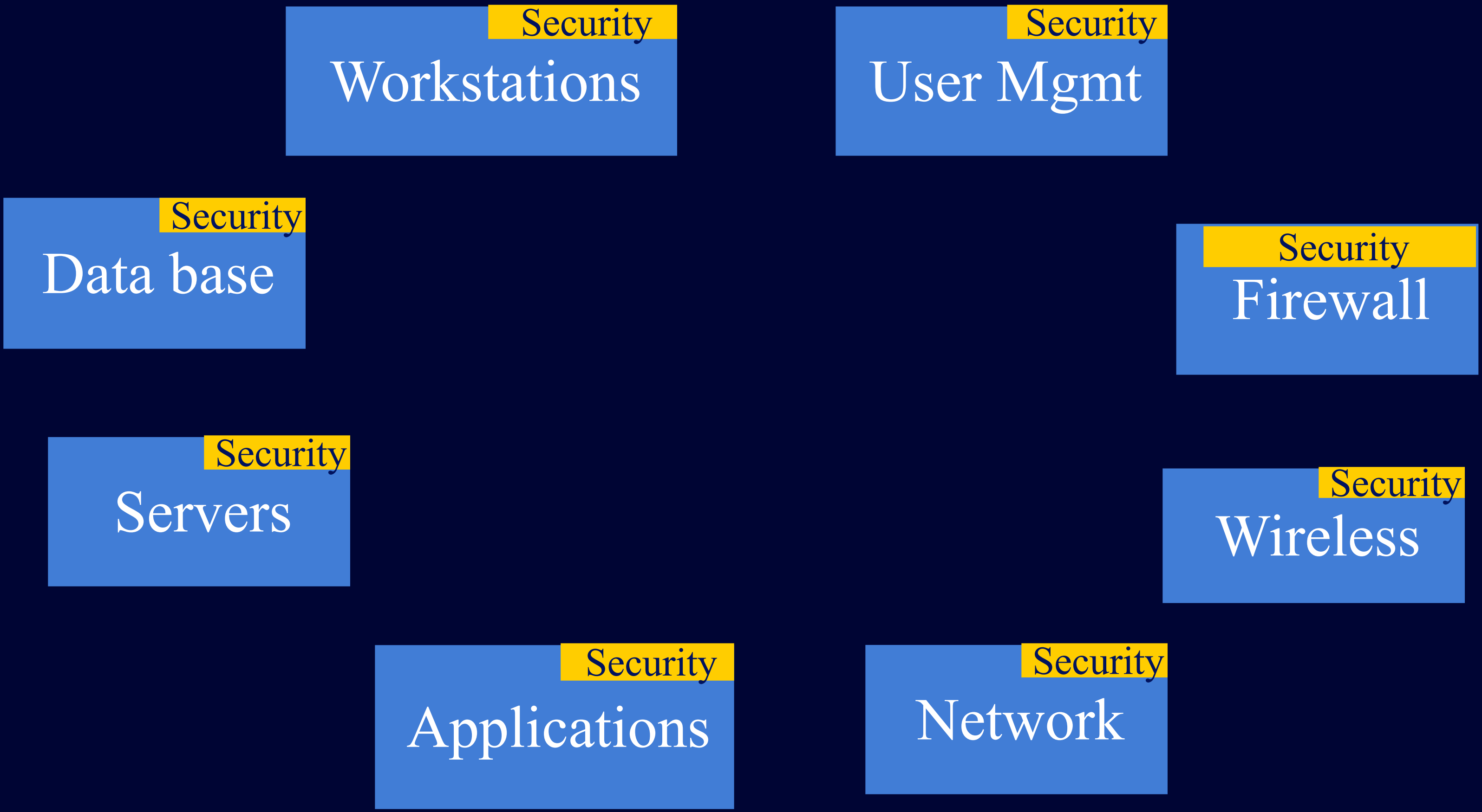
- system analysts
- application analysts
- business analysts
- technical analysts
- system administrators
- application programmers
- auditors
- IT managers
- security leads
- network leads

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



Security
Workstations

Security
User Mgmt

Security
Data base

Security
Firewall

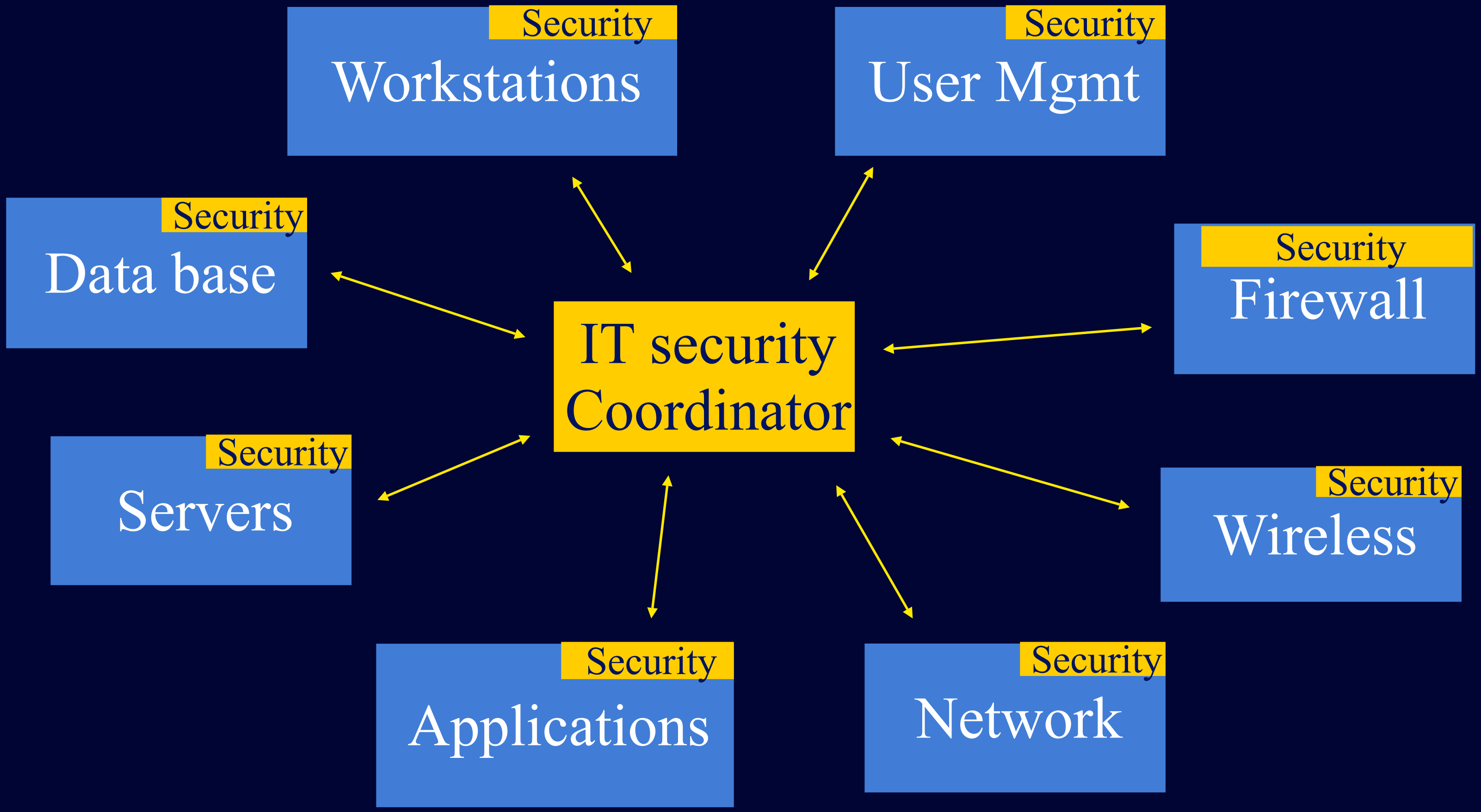
Security
Servers

Security
Wireless

Security
Applications

Security
Network

Loosely Coordinated Teams



IT security Coordinator

Security
Workstations

Security
User Mgmt

Security
Data base

Security
Firewall

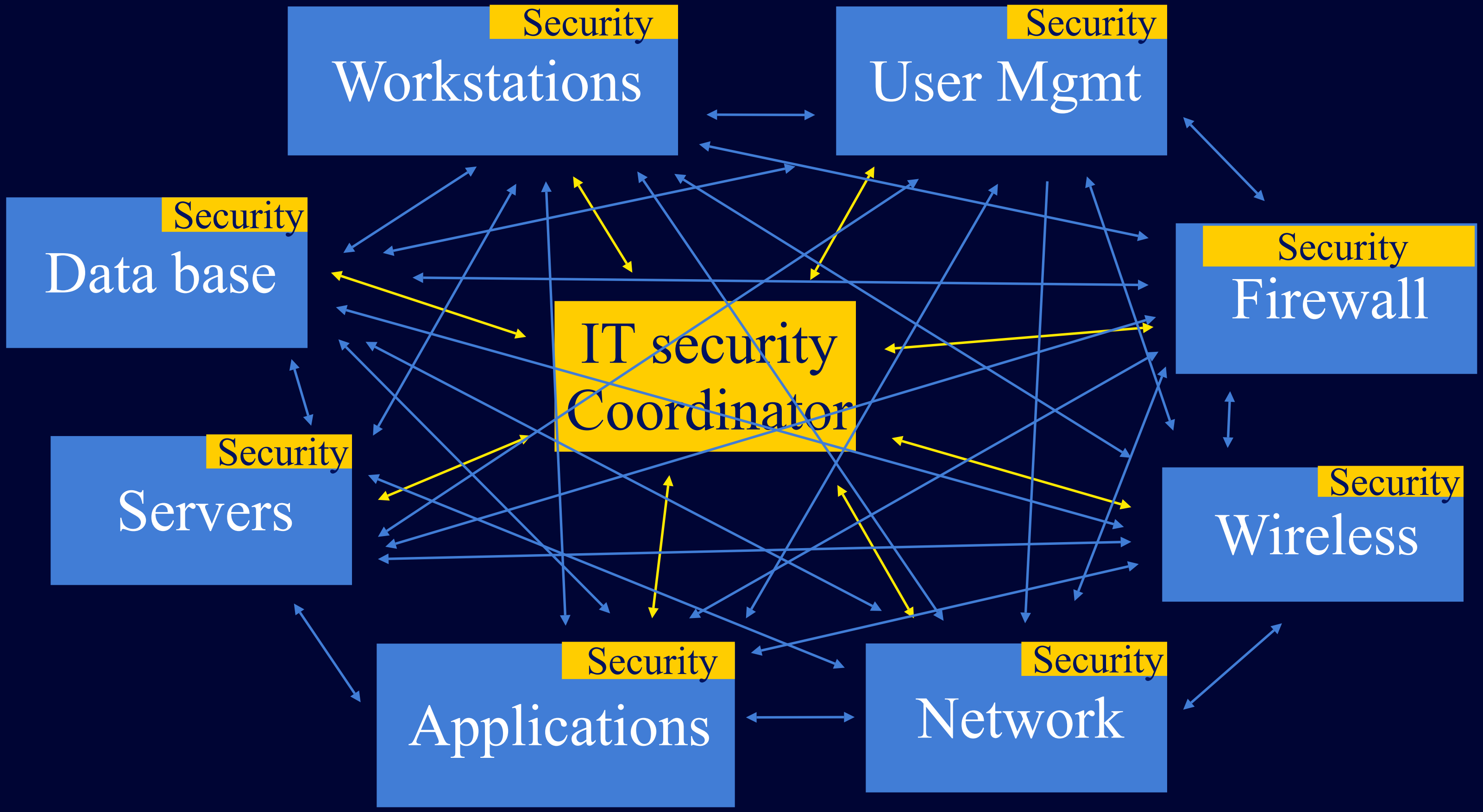
Security
Servers

Security
Wireless

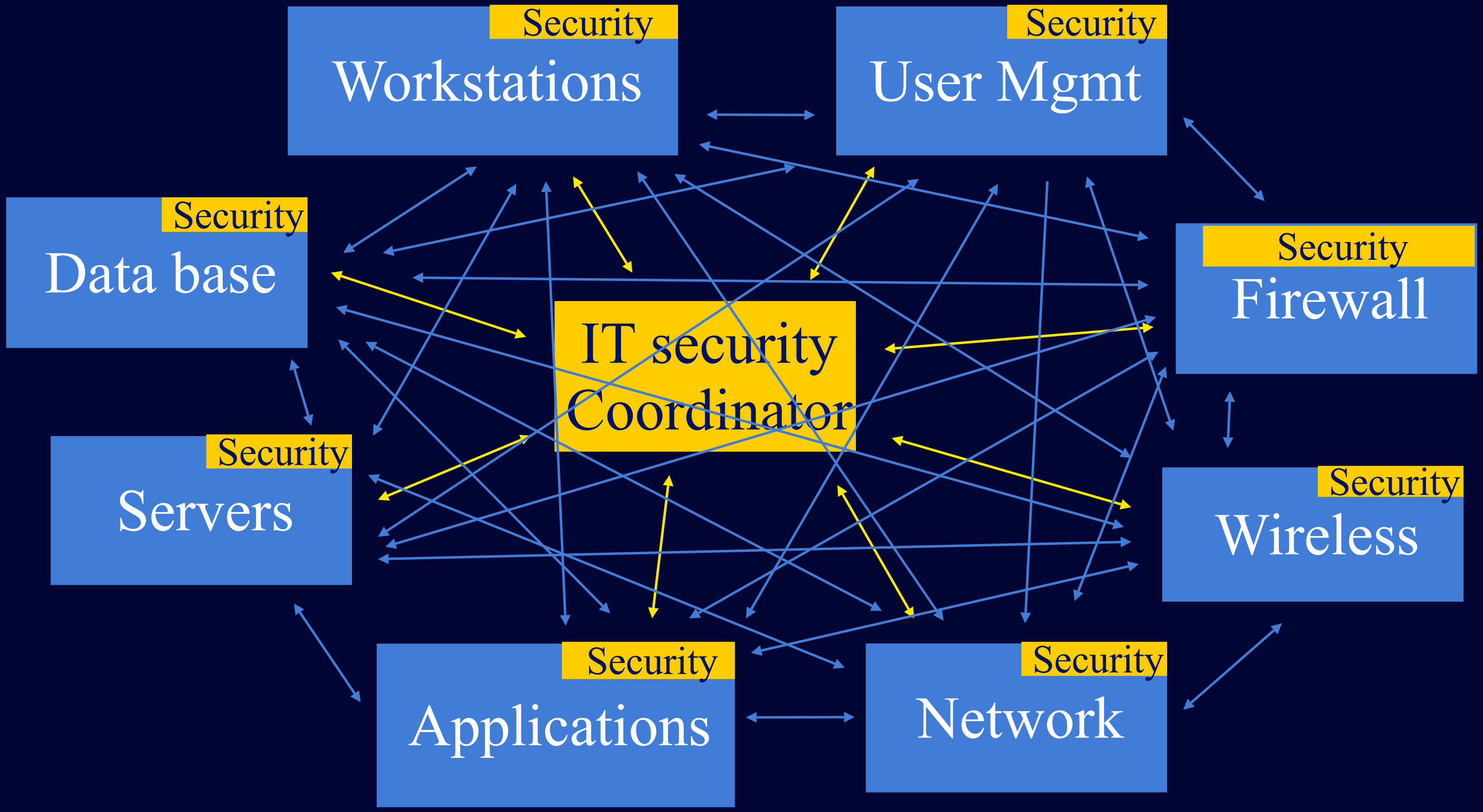
Security
Applications

Security
Network

Loosely Coordinated Teams



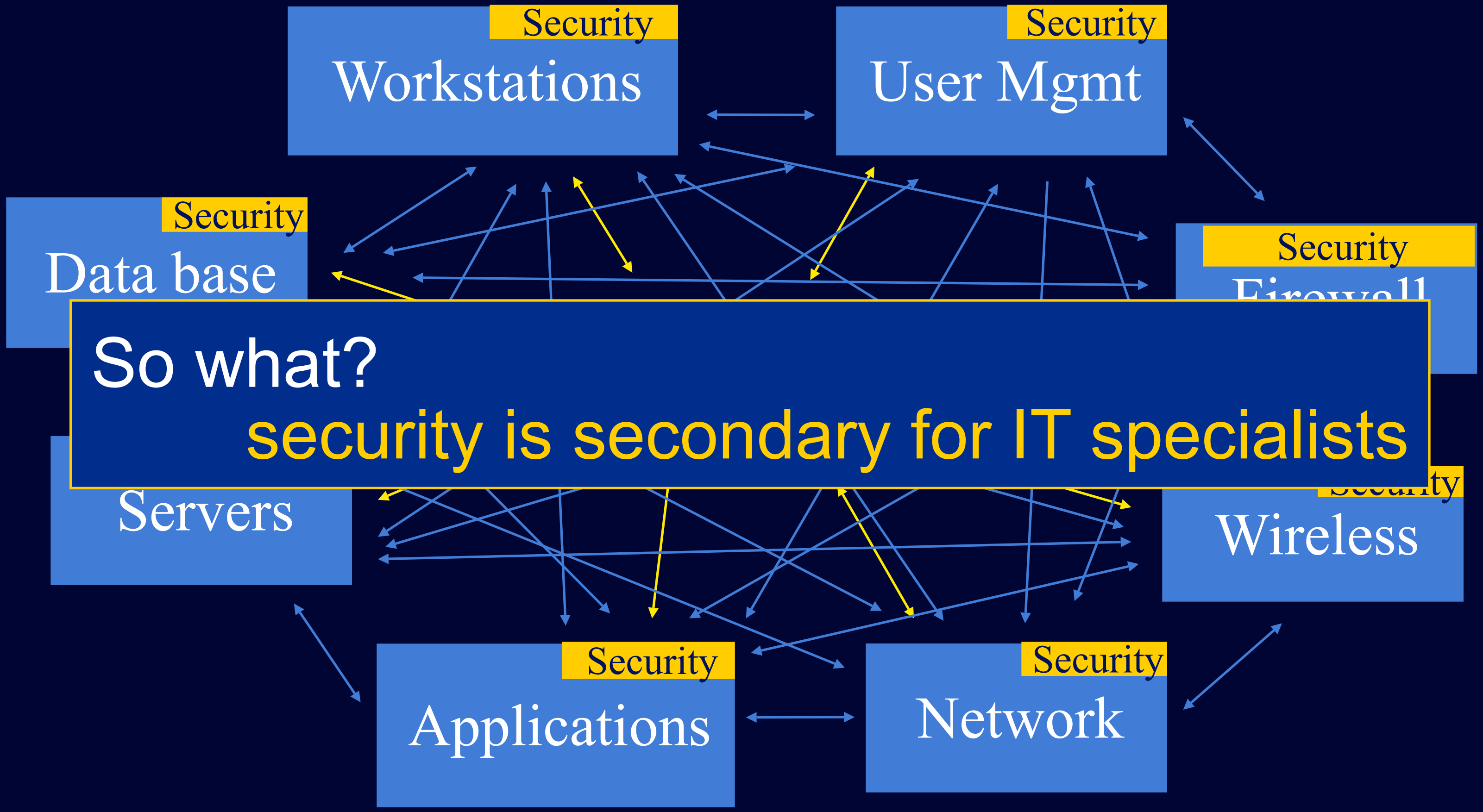
Loosely Coordinated Teams



"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

Loosely Coordinated Teams



So what?

security is secondary for IT specialists

“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

Three Main Kinds of Responsibilities

Respond

- Security incident
- Patch cycle
- Troubleshooting
- ...

Three Main Kinds of Responsibilities

Respond

- Security incident
- Patch cycle
- Troubleshooting
- …

Design

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

Three Main Kinds of Responsibilities

Respond

- Security incident
- Patch cycle
- Troubleshooting
- …

Design

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

Maintain

- Firewalls
- Legacy systems
- Records
- …

Activity Chain

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

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

Skills

- Pattern recognition
- Inferential analysis
- Tacit knowledge

Skills

- Pattern recognition
- Inferential analysis
- Tacit knowledge
- Bricolage

Skills

- Pattern recognition
- Inferential analysis
- Tacit knowledge
- Bricolage
  - Dictionary: “construction or creation from a diverse range of available things”
  - Origin: mid 20th century: French, from bricoler ‘do odd jobs, repair.’

Skills

- Pattern recognition
- Inferential analysis
- Tacit knowledge
- Bricolage
  - Dictionary: "construction or creation from a diverse range of available things"
  - Origin: mid 20th century: French, from bricoler 'do odd jobs, repair.'

So what?

- finding gaps in tool support
- tool improvement
- new usability testing methods

Skills

- Pattern recognition
- Inferential analysis
- Tacit knowledge
- Bricolage
  - 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.

So what?

- finding gaps in tool support
- tool improvement
- new usability testing methods

Theme: IT Security vs. General IT

Tasks & Tools

IT Security vs. General IT

Challenges

Interactions

Errors

Management Model

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”

Study Participant

Perception and Environment

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"

Study Participant

SPs need broader external scope than general IT

Legislation (e.g., Sarbanes Oxley)

Model of Differences

Scope

Troubleshooting Complexity

Usability vs. Security Tradeoff

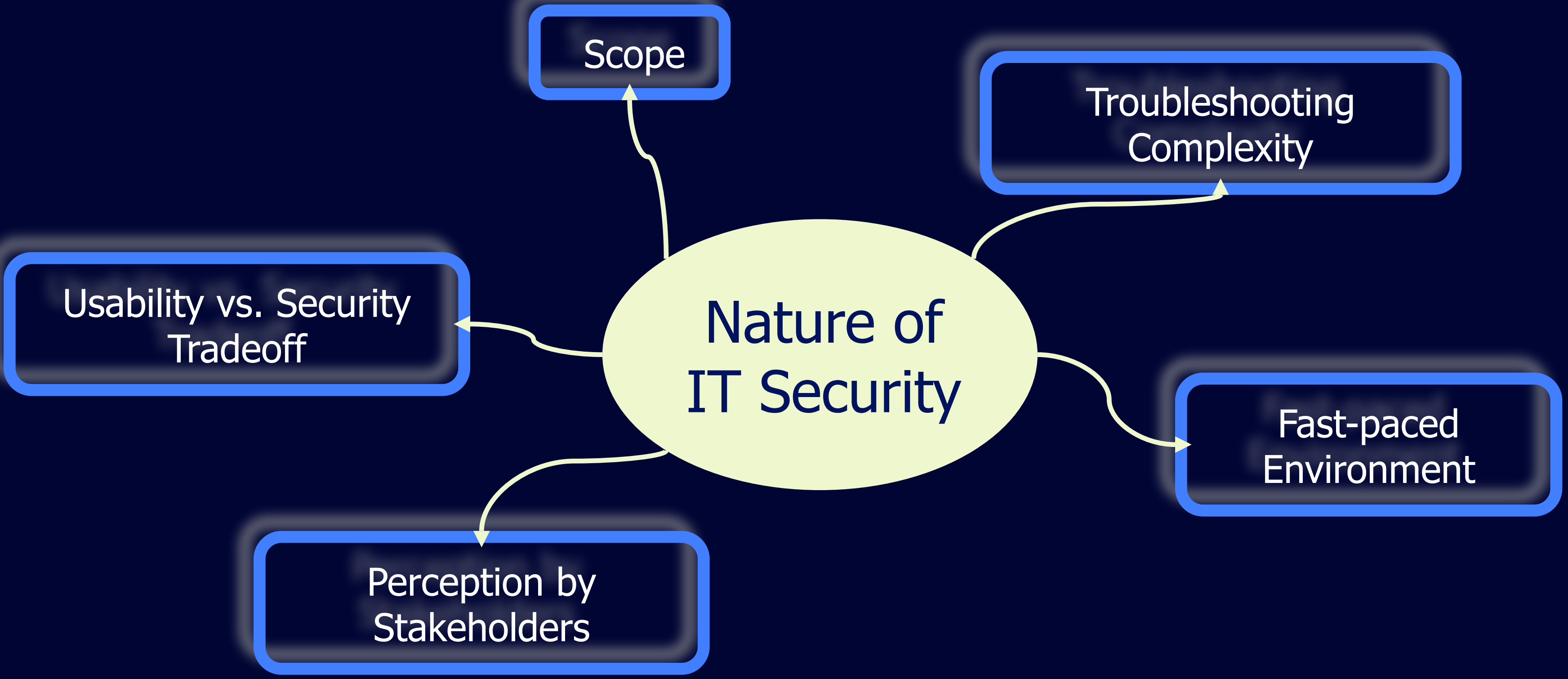
Fast-paced Environment

Perception by Stakeholders

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.

Model of Differences

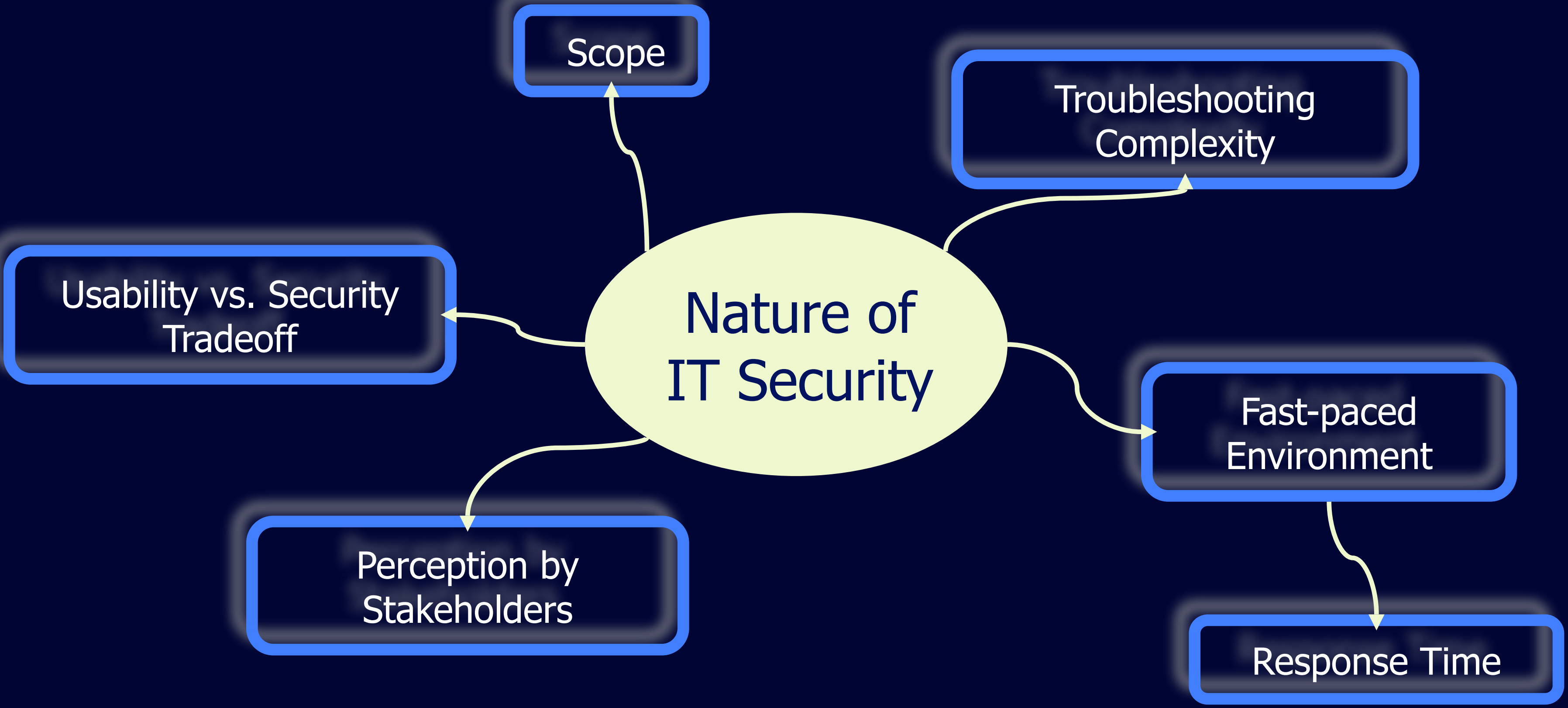


Scope
Troubleshooting Complexity
Usability vs. Security Tradeoff
Nature of IT Security
Fast-paced Environment
Perception by Stakeholders

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.

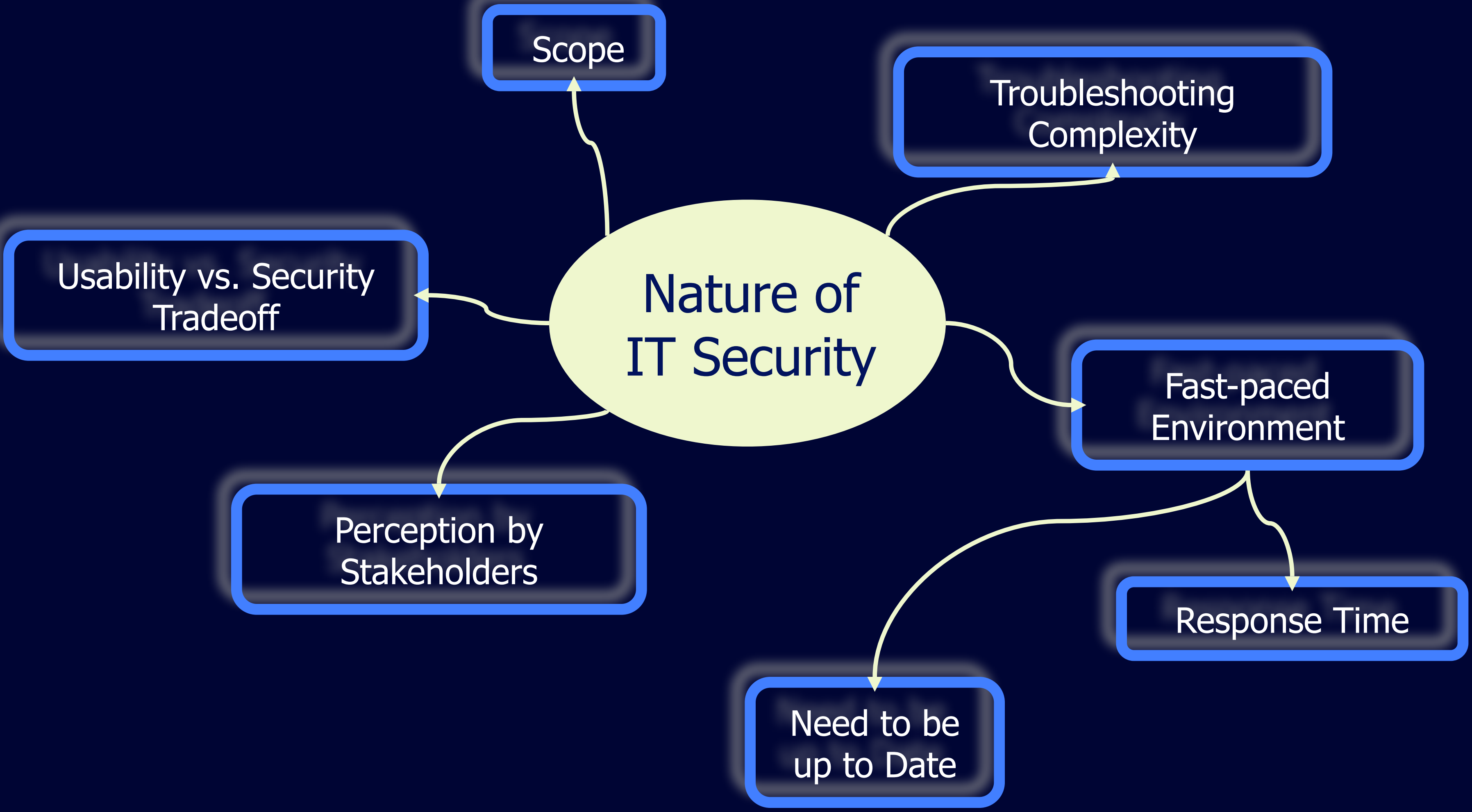
Model of Differences


Scope
Troubleshooting Complexity
Usability vs. Security Tradeoff
Nature of IT Security
Fast-paced Environment
Perception by Stakeholders
Response Time

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.

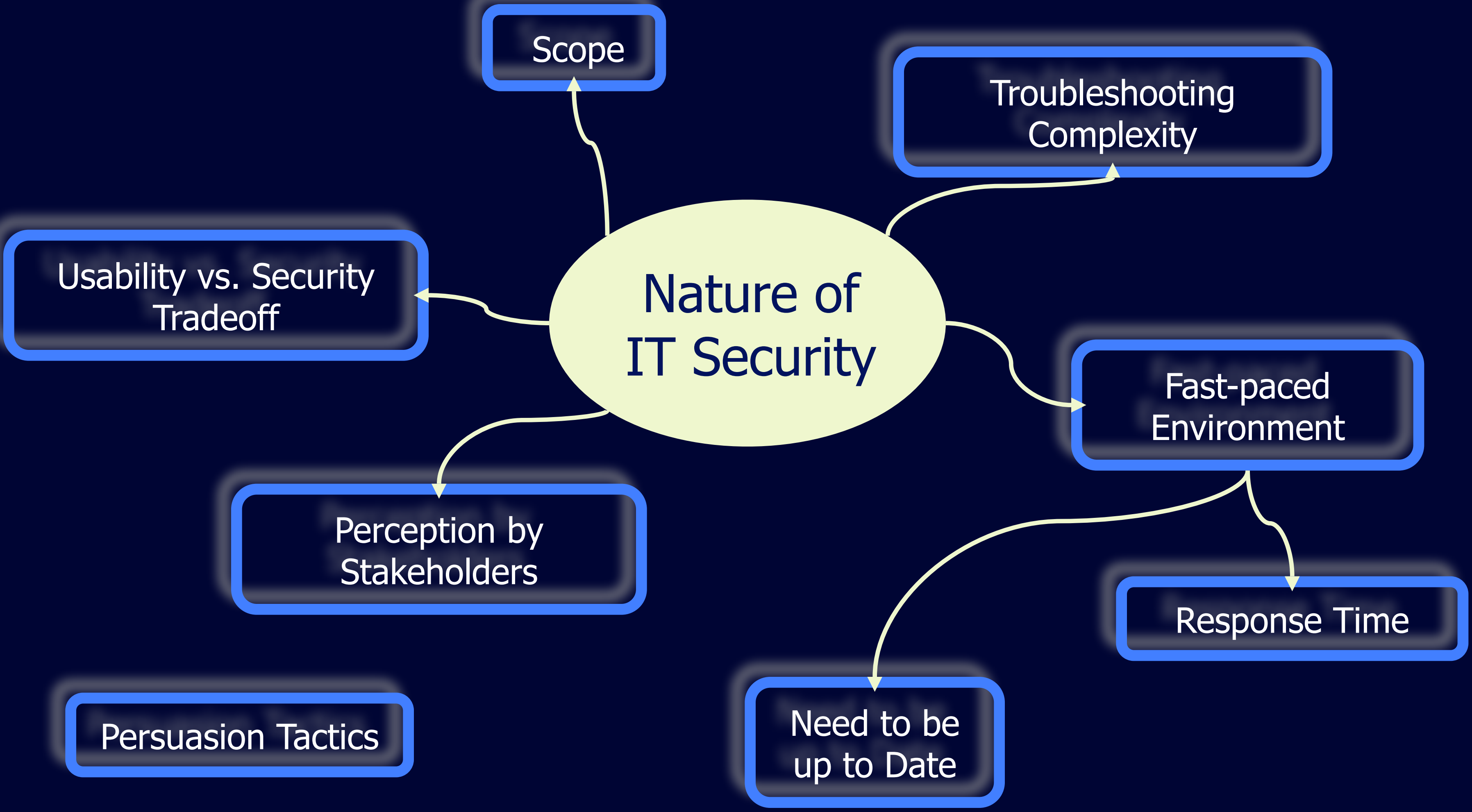
Model of Differences


Scope
Troubleshooting Complexity
Usability vs. Security Tradeoff
Nature of IT Security
Fast-paced Environment
Perception by Stakeholders
Response Time
Need to be up to Date

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.

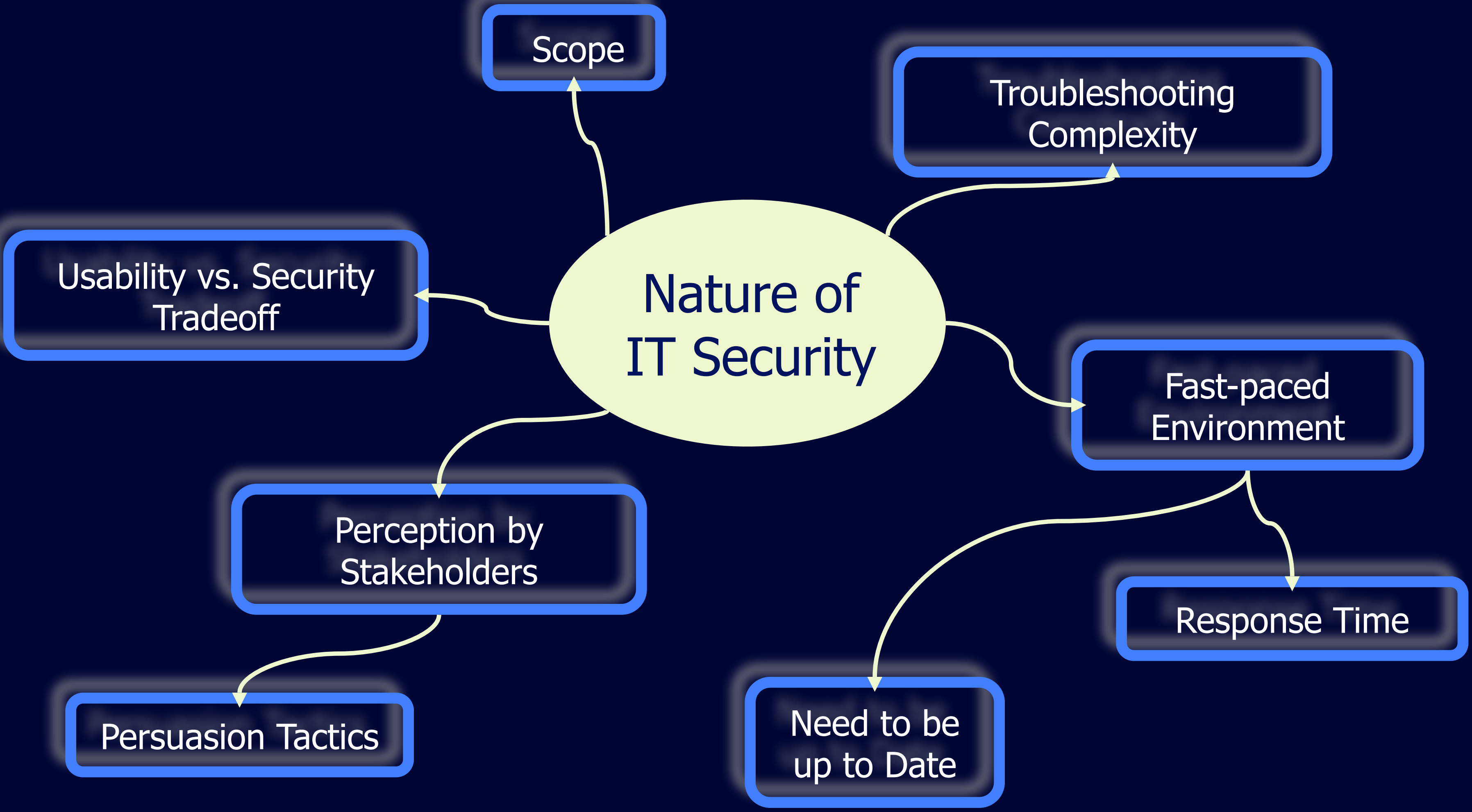
Model of Differences



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.

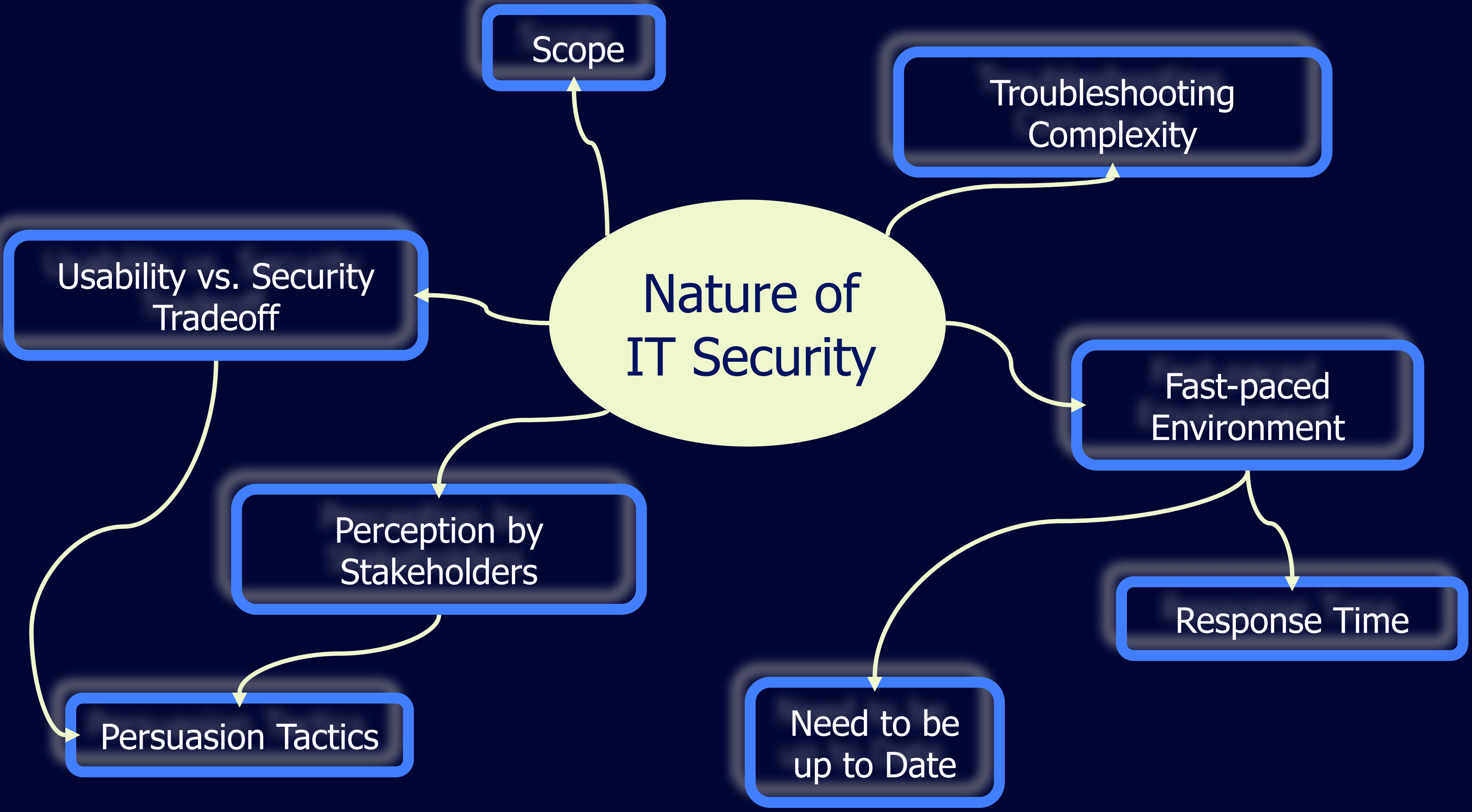
Model of Differences



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.

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.

Theme: Challenges

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

Theme: Challenges

Tasks & Tools

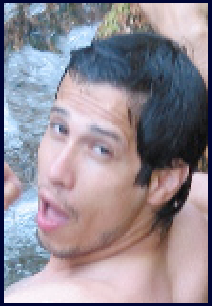
IT Security vs. General IT

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

Challenges: Technological

- Vulnerabilities

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

Challenges: Human

- Culture
  - Poor security practices result in difficulties to implement security controls
- Training
  - SPs lack the necessary training

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
- Business Relationships
- Security Low Priority
- Task Distribution
- Open Environment
- Tight Schedules
- Data Access
- Budget

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

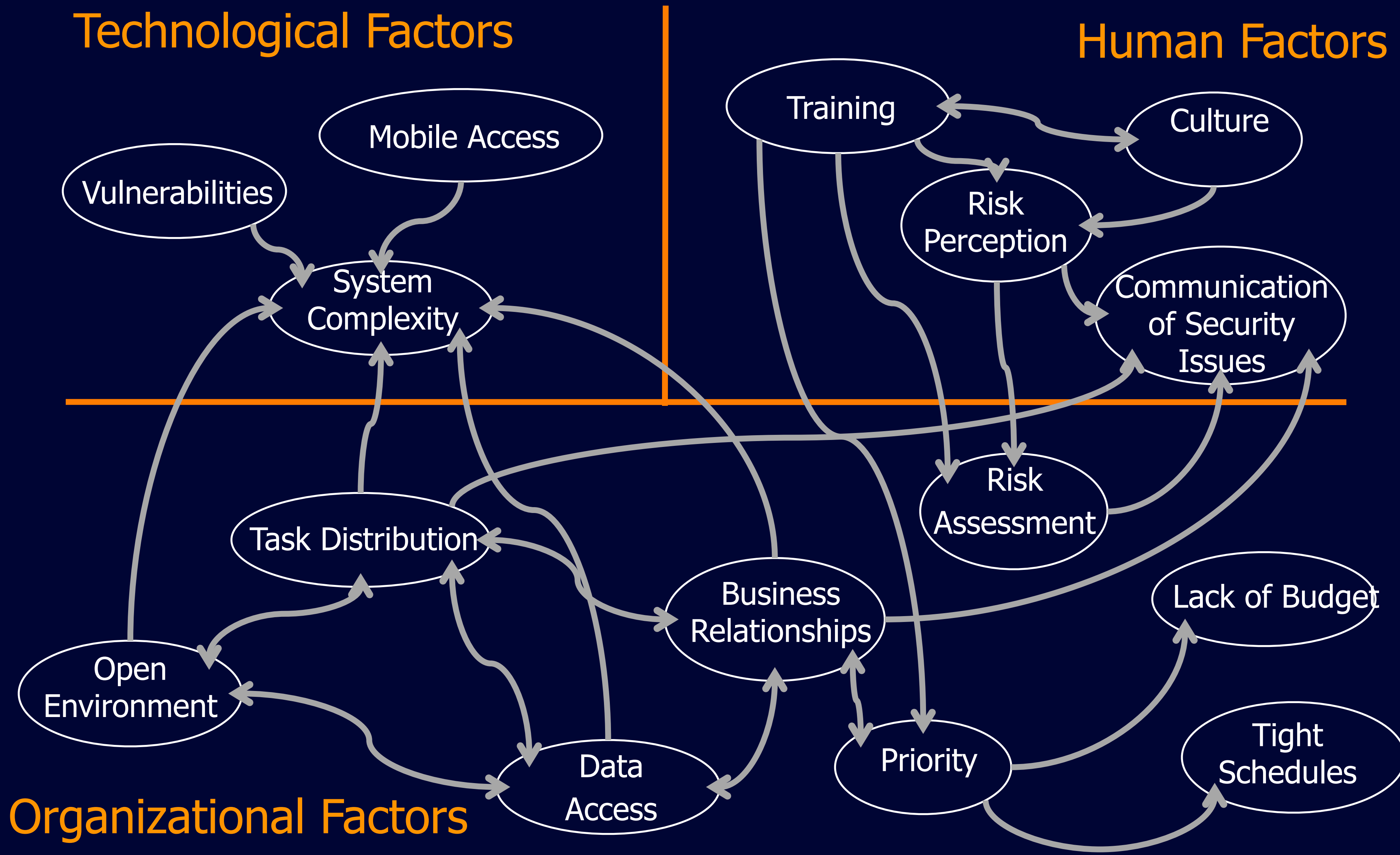
Distribution of responsibilities was an issue: “the decentralized nature does not help”…

Open Environment

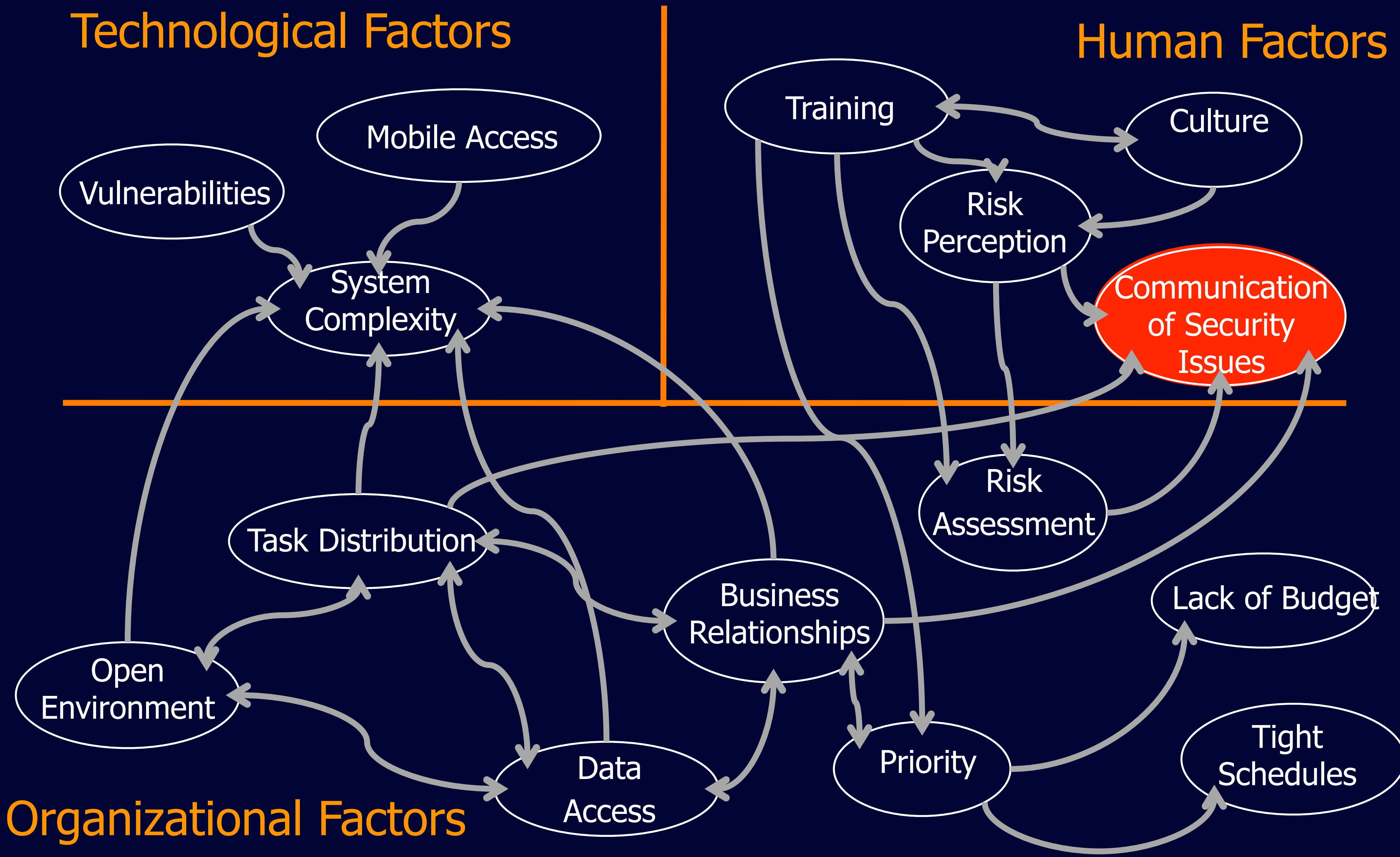
Tight Schedules

Data Access

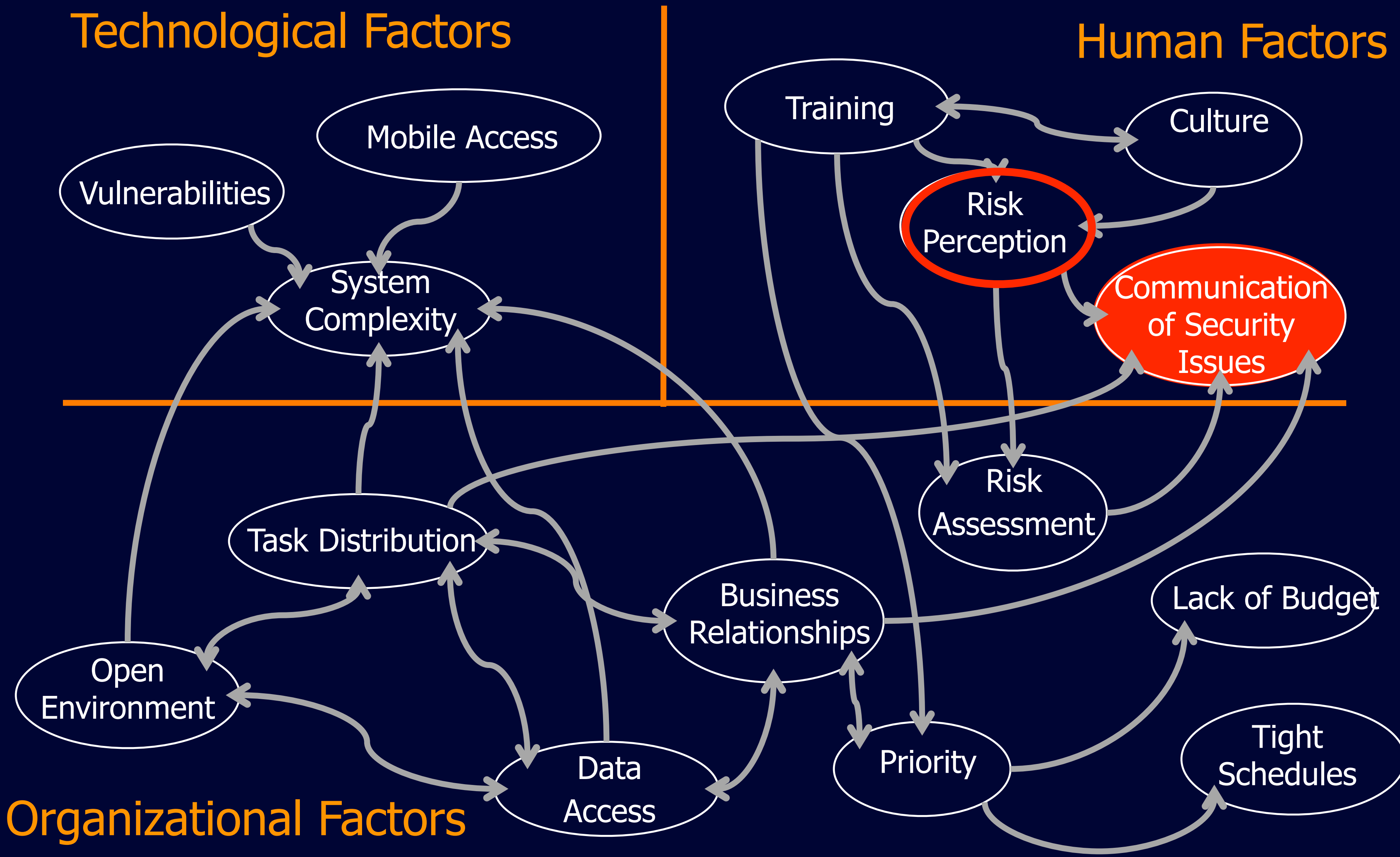
Budget



R. Werlinger, K. Hawkey, K. Beznosov, “Human, Organizational and Technological Challenges of Implementing IT Security in Organizations”, 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.



Technological Factors

Human Factors

Organizational Factors

Mobile Access

Vulnerabilities

System Complexity

Training

Culture

Risk Perception

Communication of Security Issues

Risk Assessment

Task Distribution

Business Relationships

Lack of Budget

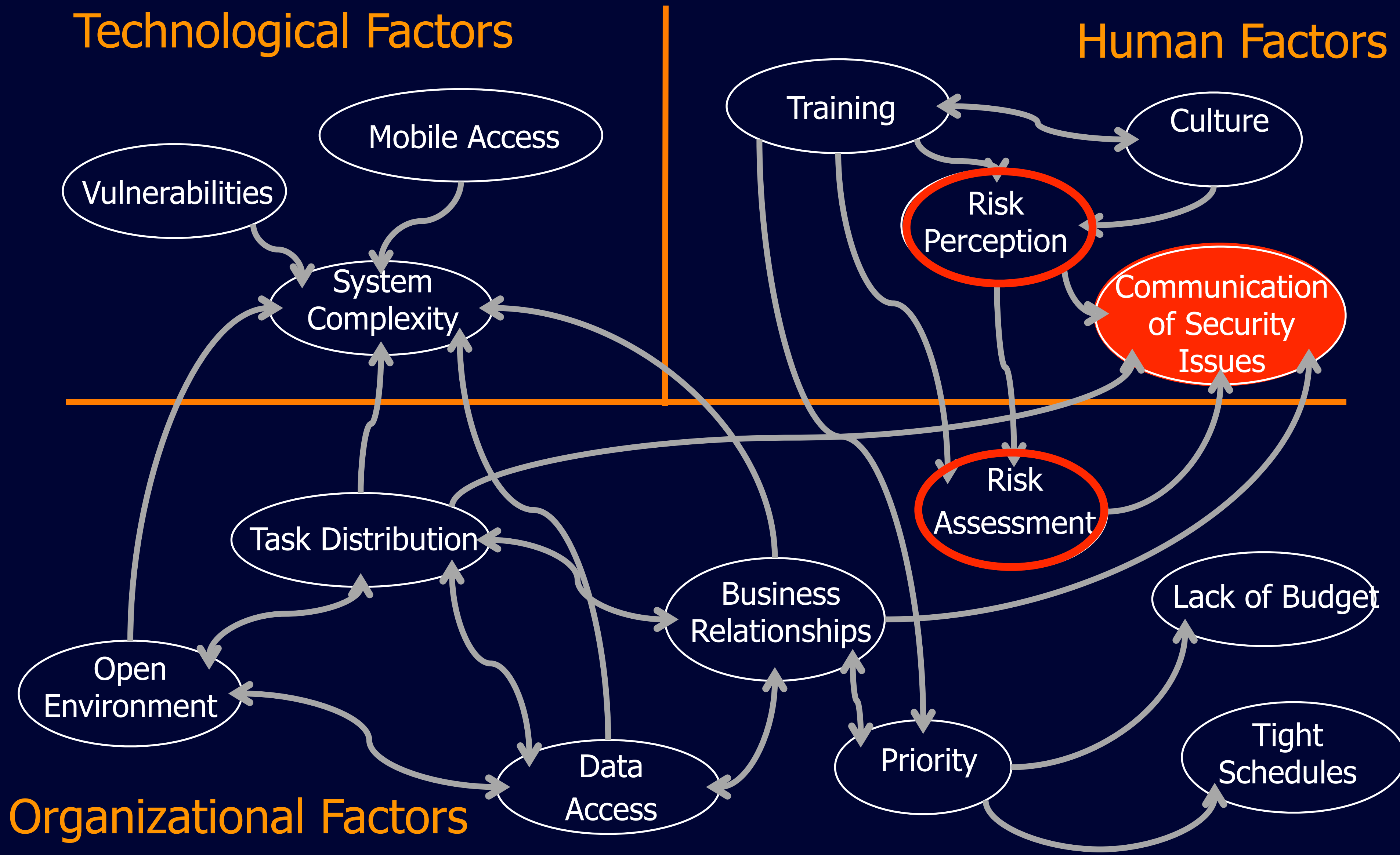
Open Environment

Data Access

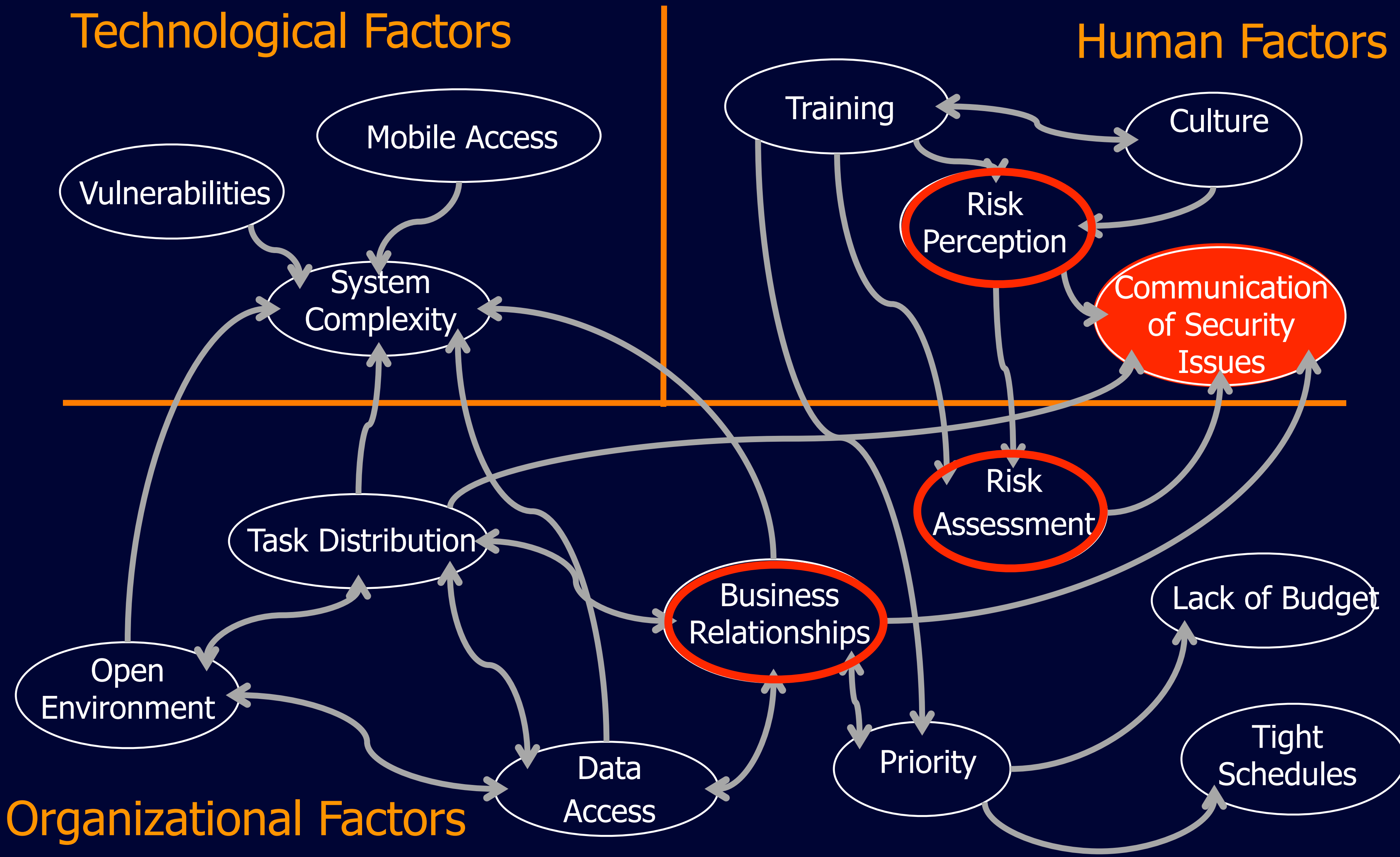
Priority

Tight Schedules

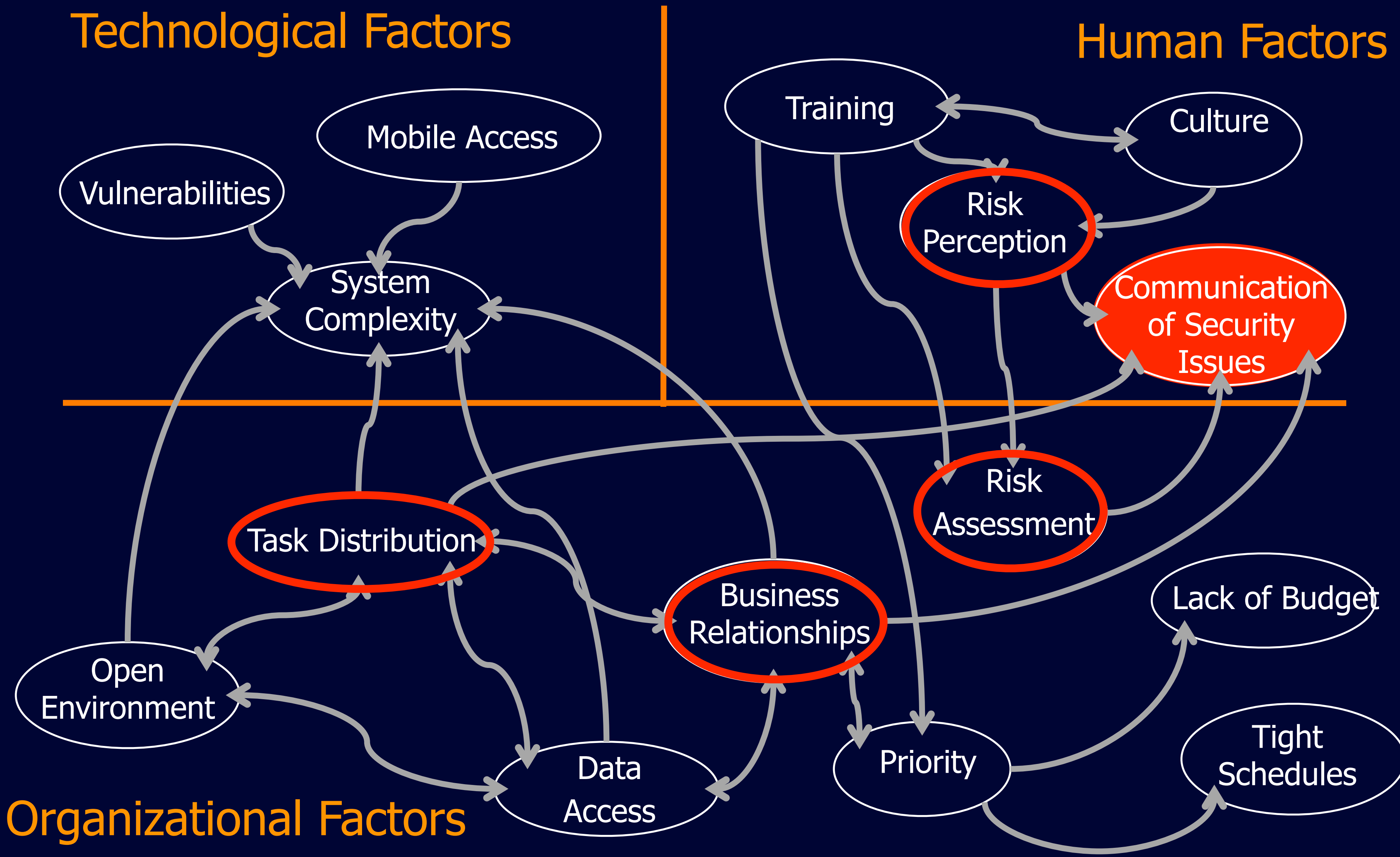
R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.



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.



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.



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.

Theme: IT Security vs. General IT

Tasks & Tools

IT Security vs. General IT

Challenges

Interactions

Errors

Management Model

Theme: IT Security vs. General IT

Tasks & Tools

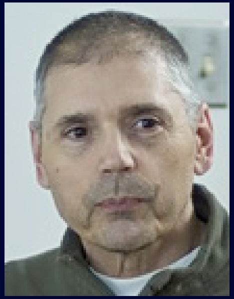
IT Security vs. General IT

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

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

- 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

Suboptimal Situations

Distributed and complex nature of IT security management

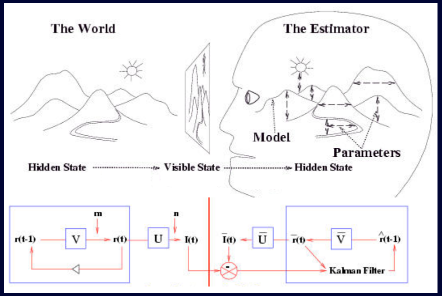
Suboptimal situations, i.e., errors

- 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

Summary

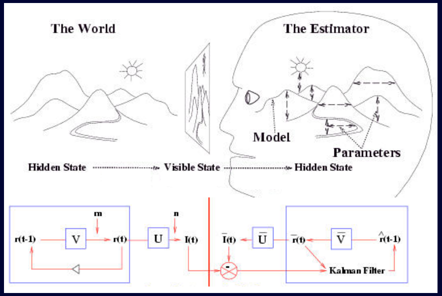
Field study



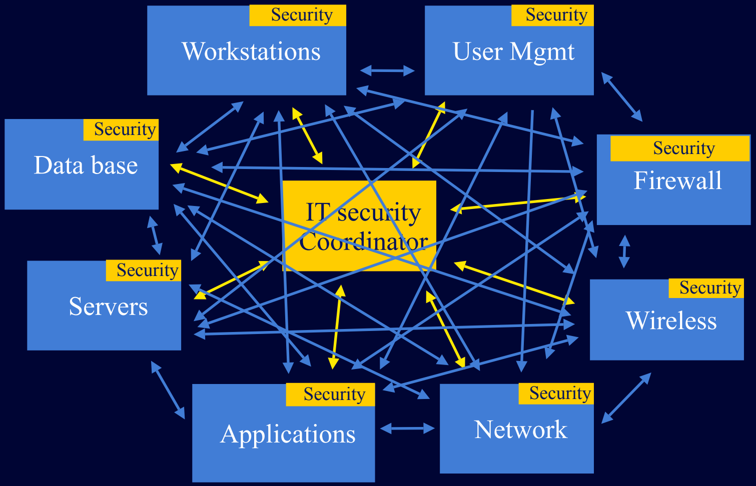
Models

Summary

Field study



Models



Security Workstations

Security User Mgmt

Security Data base

Security Firewall

IT security Coordinator

Security Servers

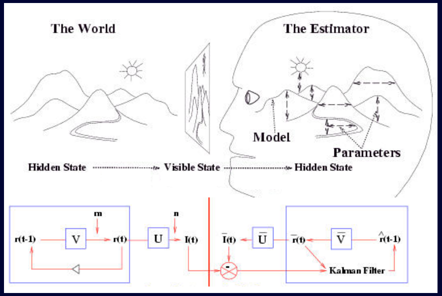
Security Wireless

Security Applications

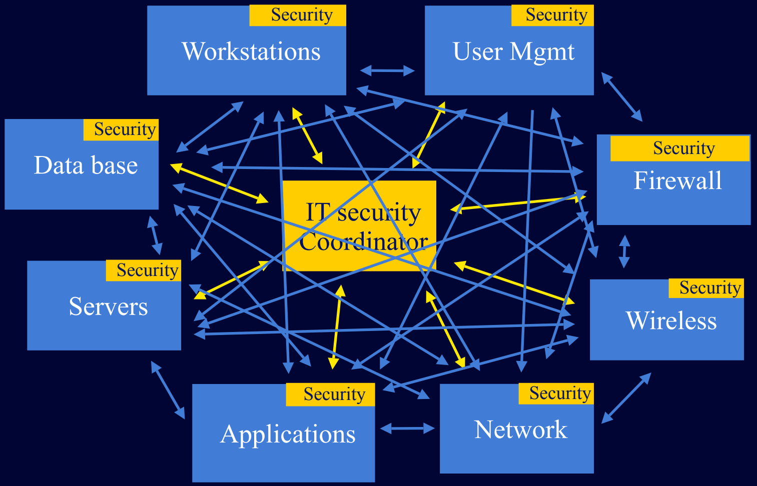
Security Network

Summary

Field study



Models



Security
Workstations

Security
User Mgmt

Security
Data base

Security
Firewall

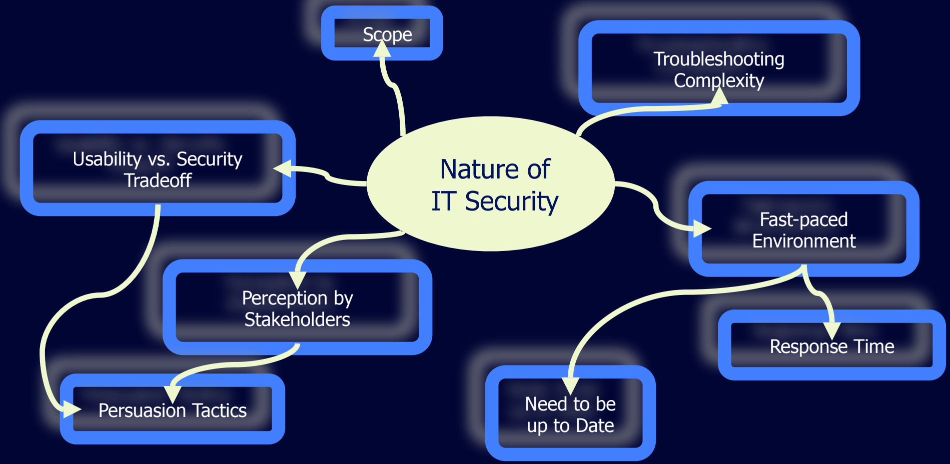
IT security
Coordinator

Security
Servers

Security
Wireless

Security
Applications

Security
Network



Nature of
IT Security

Scope

Troubleshooting
Complexity

Usability vs. Security
Tradeoff

Fast-paced
Environment

Perception by
Stakeholders

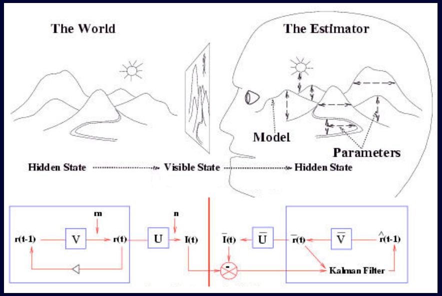
Response Time

Persuasion Tactics

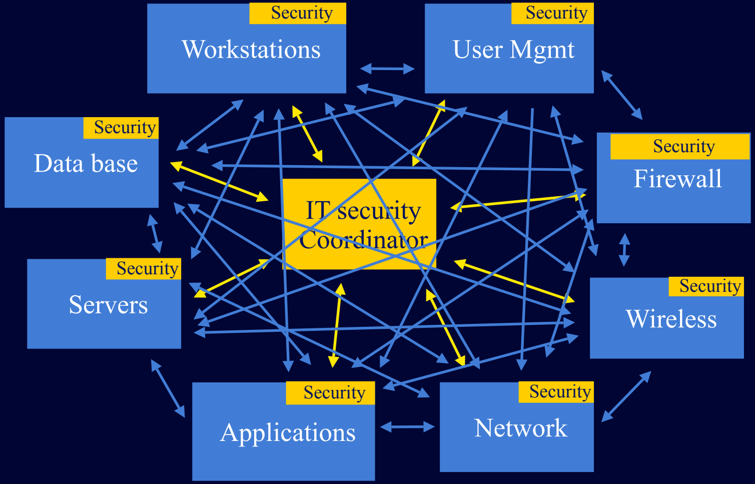
Need to be
up to Date

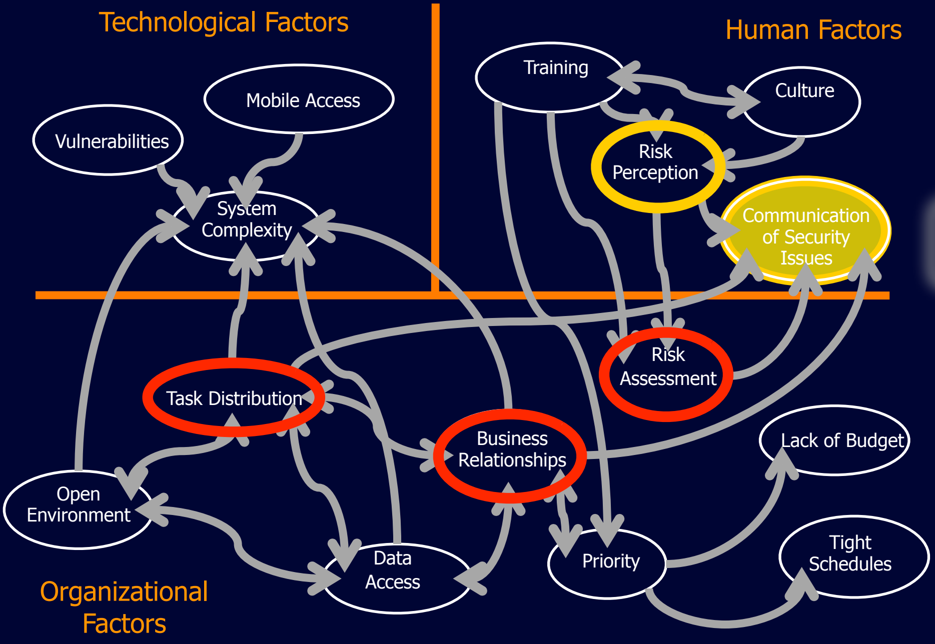
Summary

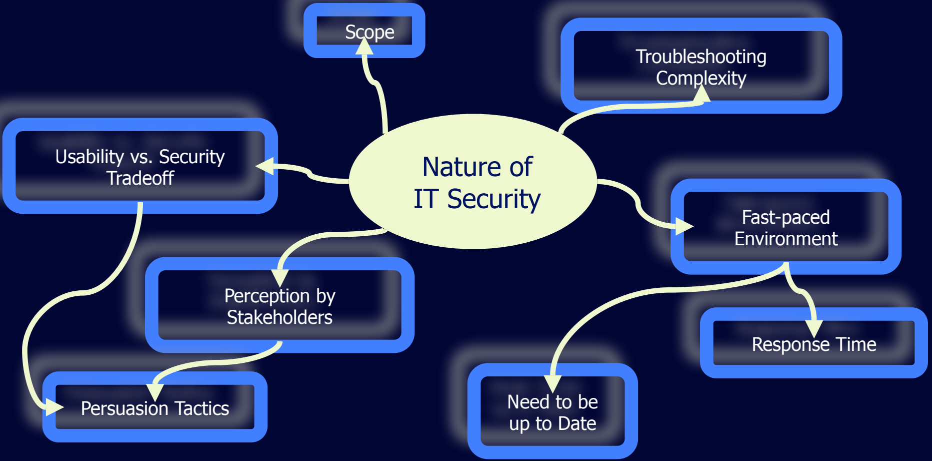
Field study



Models







Putting It All Together

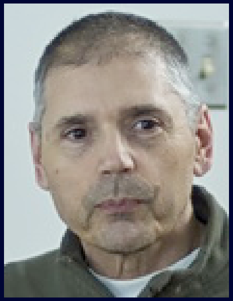
- Complexity of IT security management
- Understanding of IT security professionals
- Guidelines for tool refinements and directions for future research

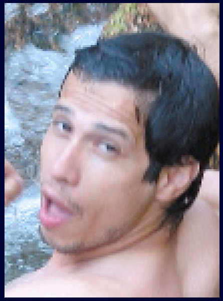
Future Challenges

- 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

Kosta Beznosov


David Botta


Rodrigo Werlinger

Kirstie Hawkey

Kasia Muldner

Sid Fels

André Gagné

Lee Iverson

Fahimeh Raja

Pooya Jaferian

Brian Fisher