Towards Understanding and Improving IT Security Management

Konstantin (Kosta) Beznosov

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering

selected publications

- P. Jaferian, H. Rashtian, K. Beznosov, “To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations,” in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), July 2014, pp. 301-320.
- P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, K. Beznosov, “Heuristics for Evaluating IT Security Management Tools,” in Human–Computer Interaction, July 2013.
- D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, “Toward Understanding Distributed Cognition in IT Security Management: The Role of Cues and Norms,” in the International Journal of Cognition, Technology & Work, Springer, September 2010, pp. 1-14.
- R. Werlinger, K. Muldner, K. Hawkey, K. Beznosov, “Examining Diagnostic Work Practices during Security Incident Response” in the Journal of Information Management & Computer Security, Emerald, v. 18 n. 1, 2010, pp.26 - 42.
- R. Werlinger, K. Hawkey, K. Beznosov, “An Integrated View of Human, Organizational, and Technology Challenges in IT Security Management,” in the Journal of Information Management & Computer Security, Emerald, v. 17, n. 1, January 2009, pp. 4-19.
- R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, K. Beznosov “The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?” in Proceedings of the SOUPS, Pittsburgh, PA, 23-25 July 2008.
- A. Gagné, K. Muldner, K. Beznosov, “Identifying Security Professionals' Needs: a Qualitative Analysis”, in *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.
- D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, “Towards understanding IT security professionals and their tools,” in *SOUPS*, pp. 100-111, Pittsburgh, PA, July 18-20 2007.
- 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.

outline

understanding

- methodology summary
- who manage IT security?
- what skills they practice?
- how are they different from others in IT?
- what challenges IDSs face?
- how they interact, responding to incidents?
- what challenges they face?
- how breakdowns in cues and norms affect ITSM?

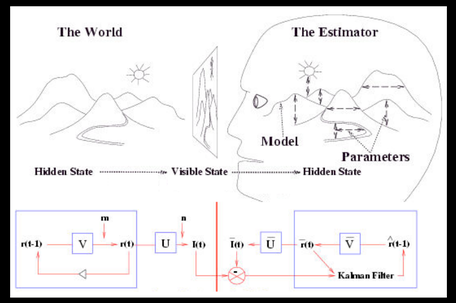
improving

- heuristics for ITSM tools design
- improving access review and certification

HOT Admin:
Human Organization and Technology Centred Improvement of IT Security Administration

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

Data Collection



Models

Techniques & Methodologies

Validation & Evaluation

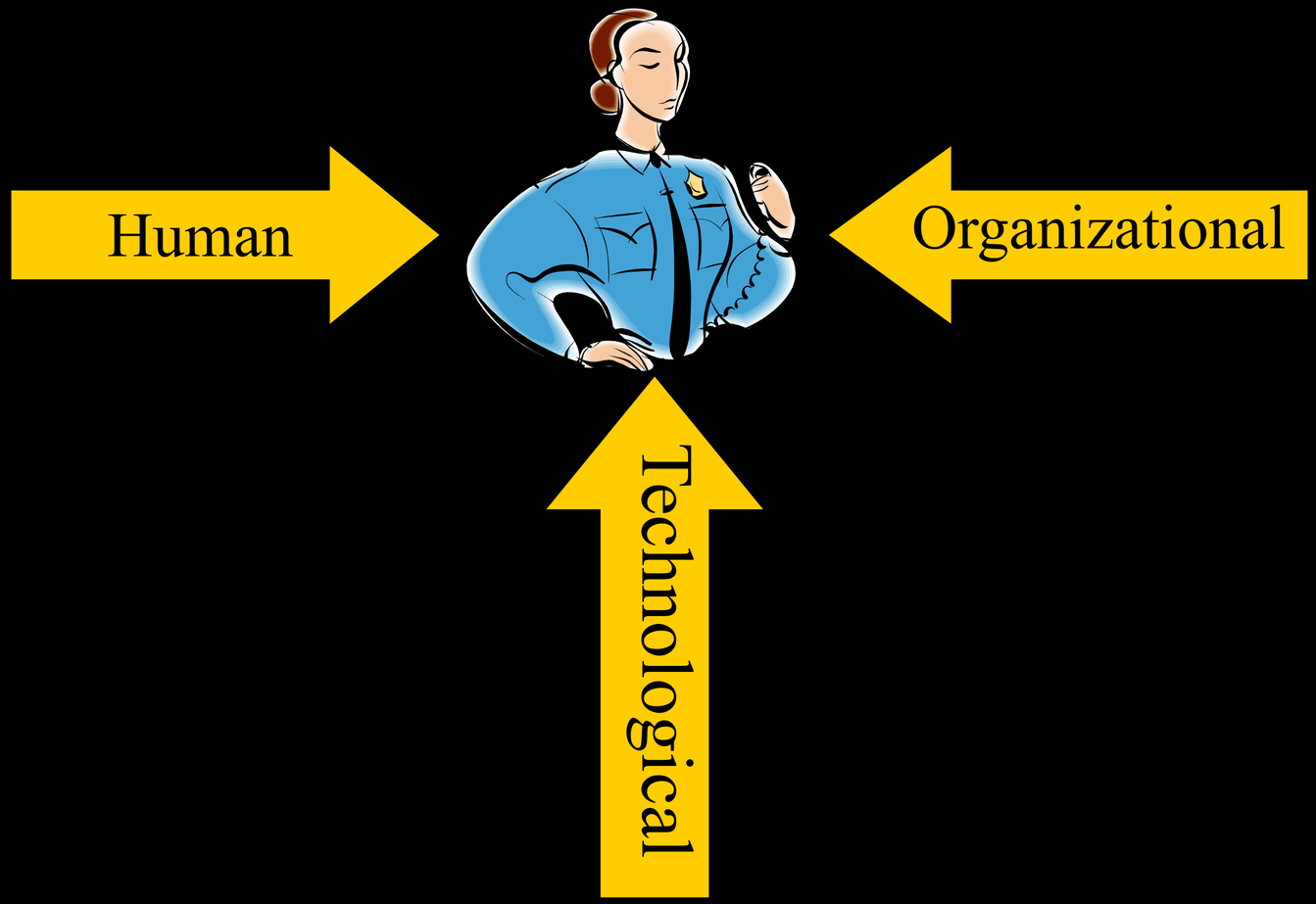
sponsors and partners

Entrust

NSERC CRSNG

SAP

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



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

recruitment

challenges

- overworked
- secrecy culture
- backstage

approaches

- professional contacts
- practical benefits
- gradual recruitment
- gatekeepers

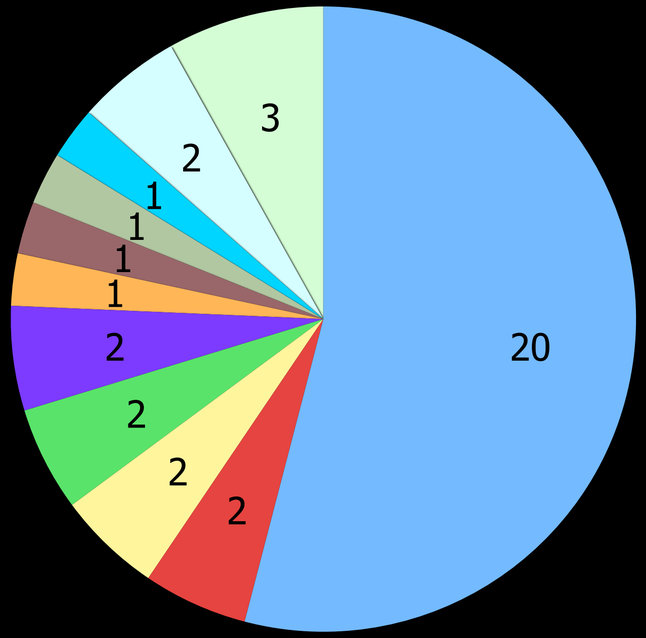
"Hello... I'm sorry but I must decline this opportunity. *We don't discuss our security administration with anyone other than with the owners of the resources we're securing*."

IT security manager who declined access to his department

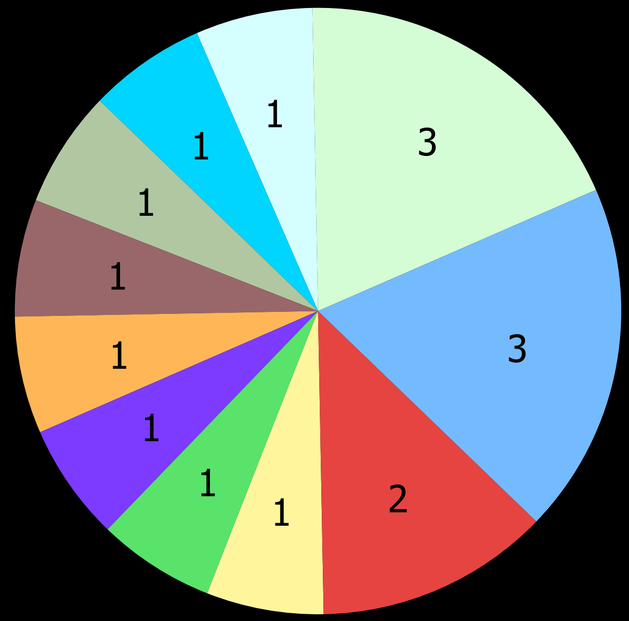
36 interviews with 36 participants between July 2006 and May 2008

industry sectors

36 interviews

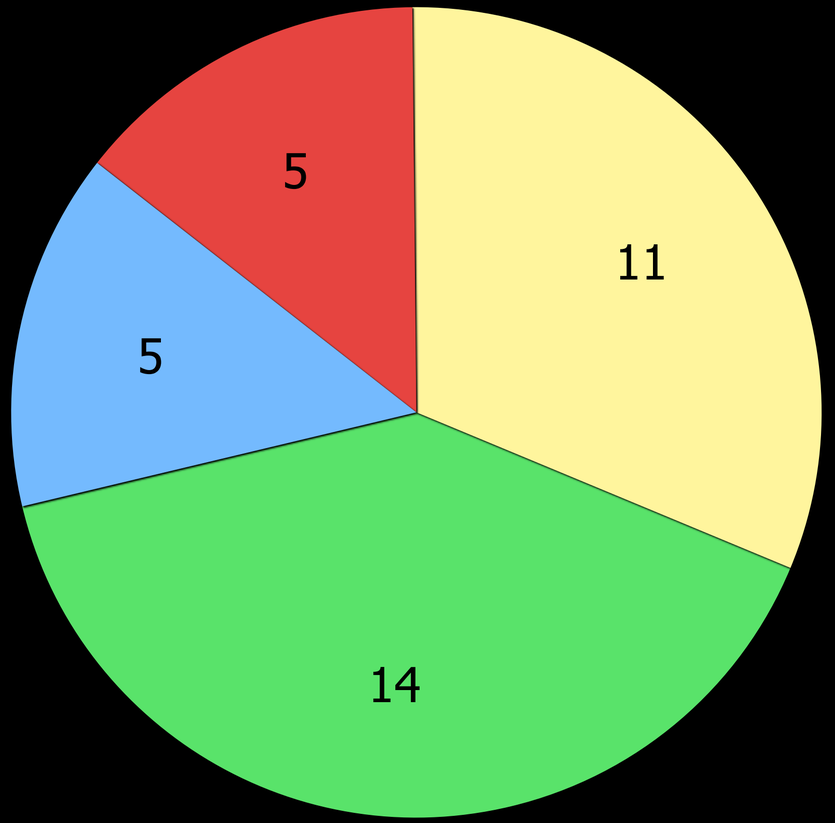


16 organizations



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

job types


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

findings

no security admins!

- system analysts
- application analysts
- business analysts
- technical analysts
- system administrators

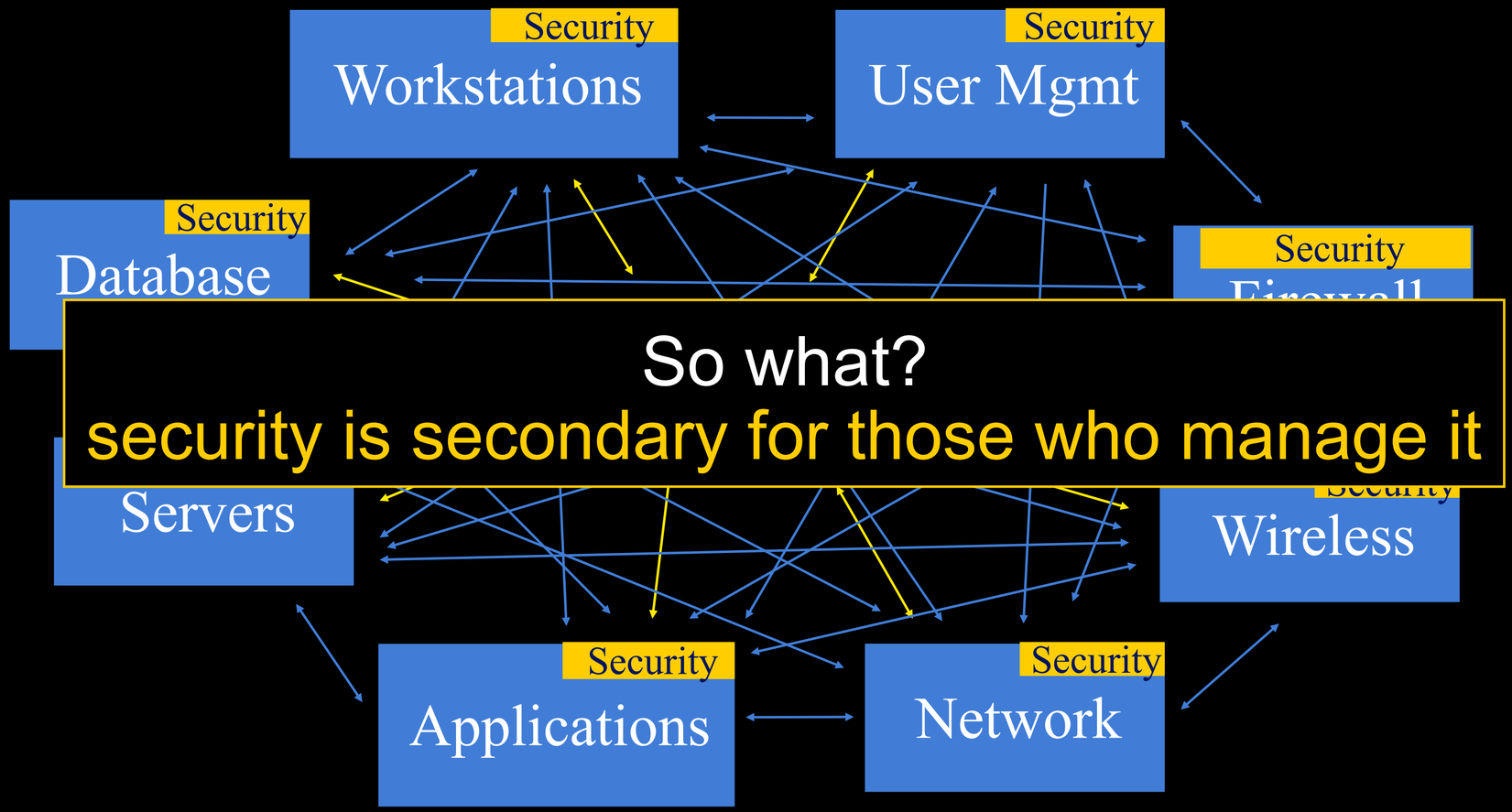
- application programmers
- auditors
- IT managers
- security leads
- network leads

``… *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*.''

Study Participant

More details in:
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.

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

More details in:

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.

skills they practice

- pattern recognition
- inferential analysis
- use of tacit knowledge
- bricolage

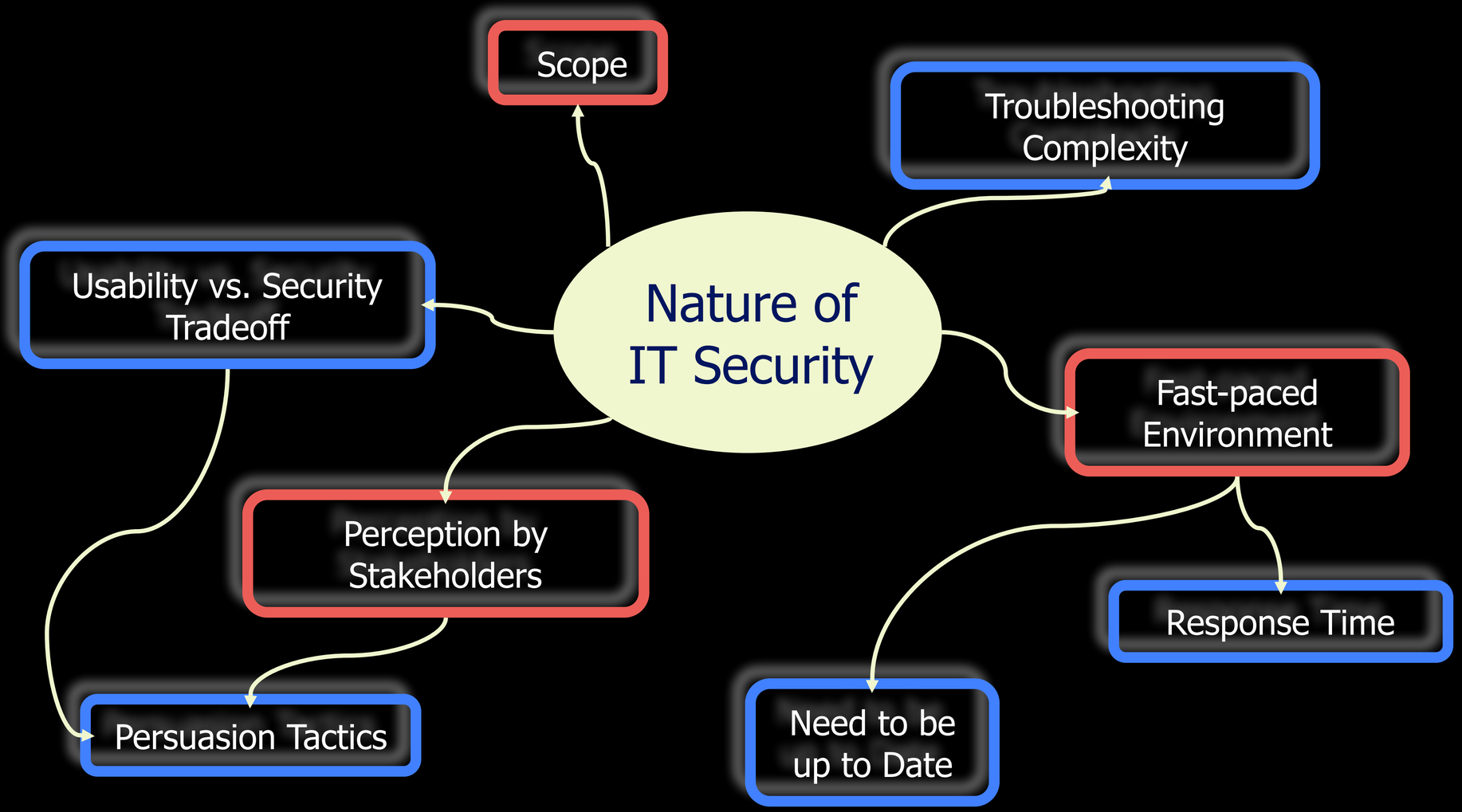
So what?

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

More details in:

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

model of differences



More details in:

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

the 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

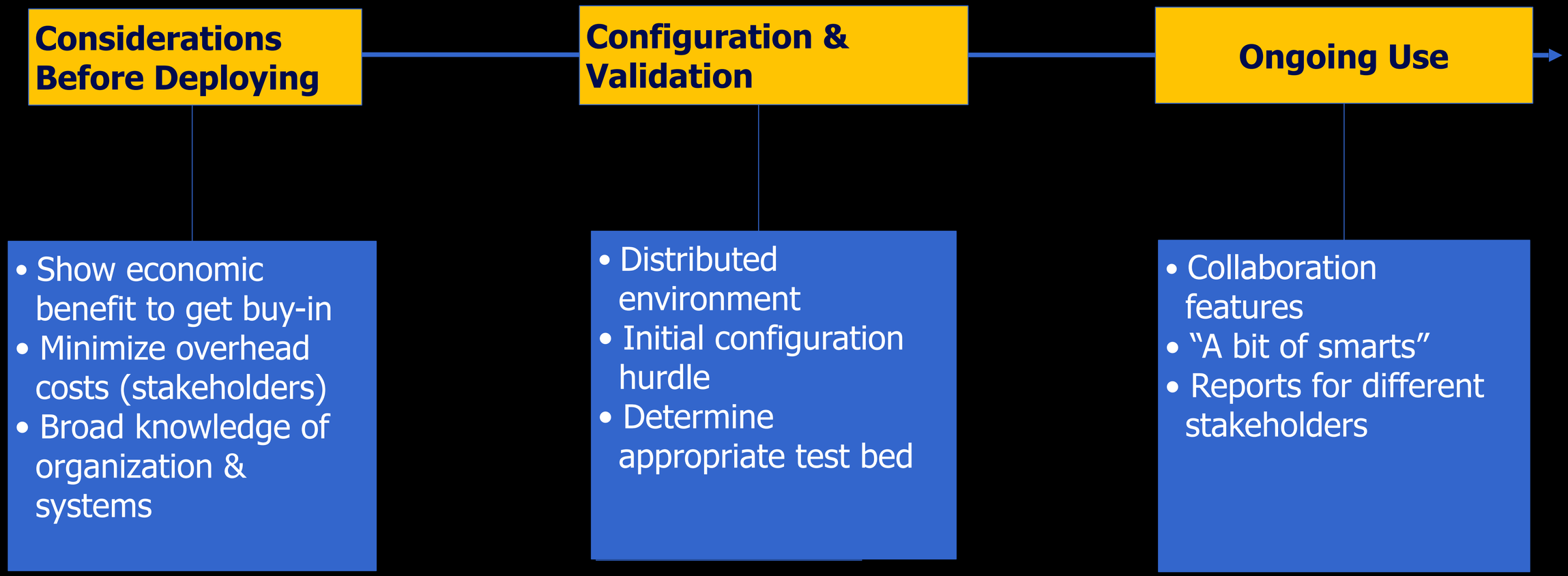
SPs need broader external scope than general IT

Legislation (e.g., Sarbanes Oxley)

More details in:

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

challenges throughout IDS deployment



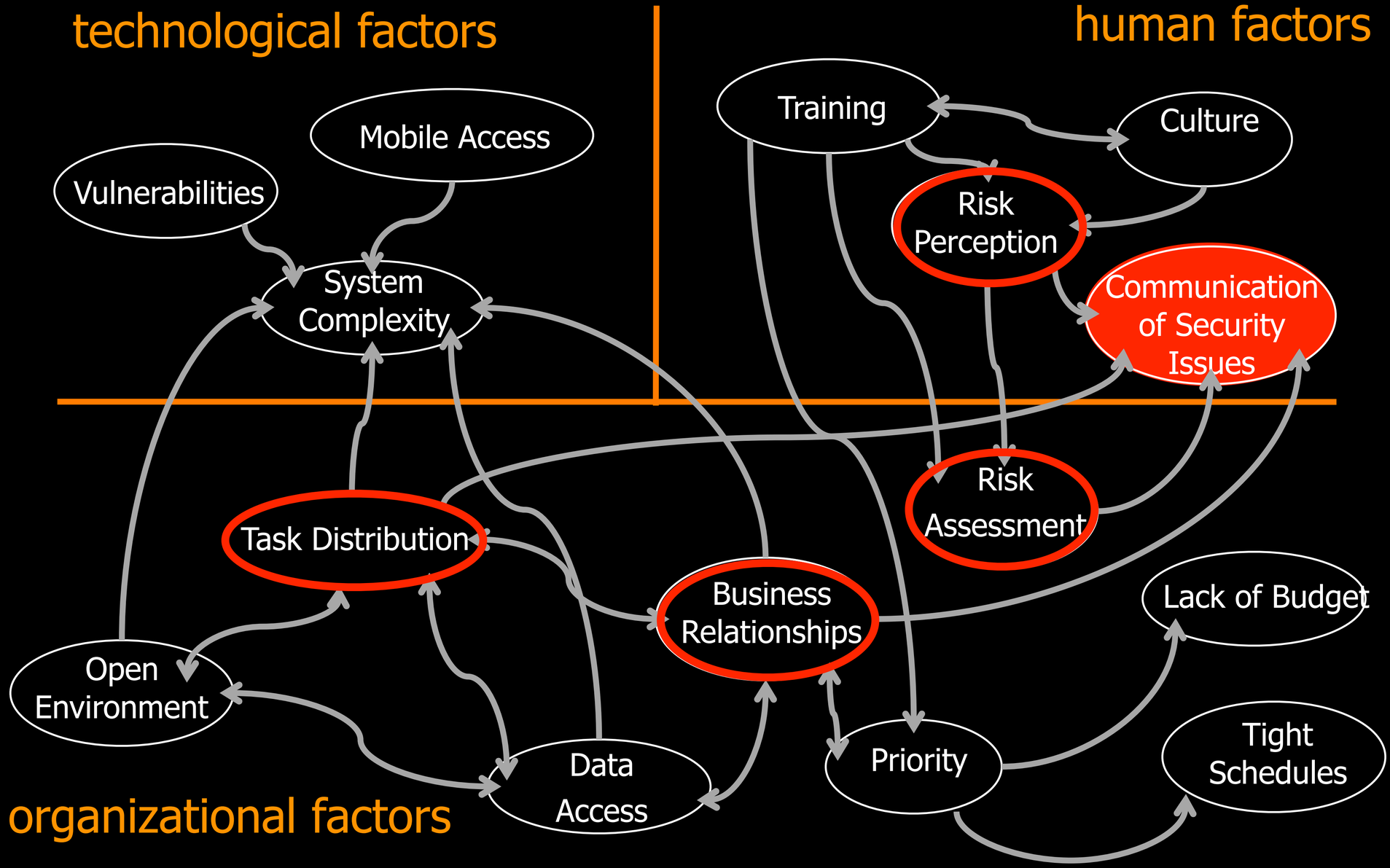
More details in:

R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, K. Beznosov "**The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?**" in the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, pp. 23-25 July 2008.

interactions during incident response

More details in:

R. Werlinger, K. Hawkey, D. Botta, K. Beznosov, “Security practitioners in context: Their activities and interactions with other stakeholders within organizations,” International Journal of Human Computer Studies, Elsevier, v.6, n.7, March 2009, pp 584-606.



More details in:
R. Werlinger, K. Hawkey, K. Beznosov, "**An Integrated View of Human, Organizational, and Technology Challenges in IT Security Management**," Journal of Information Management & Computer Security, Emerald, v. 17, n. 1, January 2009, pp. 4-19.

distributed cognition & transactive memory

- **distributed cognition** is concerned with solving problems by collaboration, where none of the collaborators individually can have a full appreciation of the problem. (Busby 2001)

- distributed cognition involves (Busby 2001)
  - **cues**: signals or clues, which participants use to determine when to act and how to act
  - **norms**: standards or patterns regarded as typical, which help make participants' subtasks consistent with each other

- **Transactive memory** is a type of mutual understanding where people in a group know who is responsible for what, and is based on the "idea that individual members can serve as external memory aids to each other" (Wegner, 1986).

More details in:
D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, "**Toward Understanding Distributed Cognition in IT Security Management: The Role of Cues and Norms**," in the International Journal of Cognition, Technology & Work, Springer, September 2010, pp. 1-14.

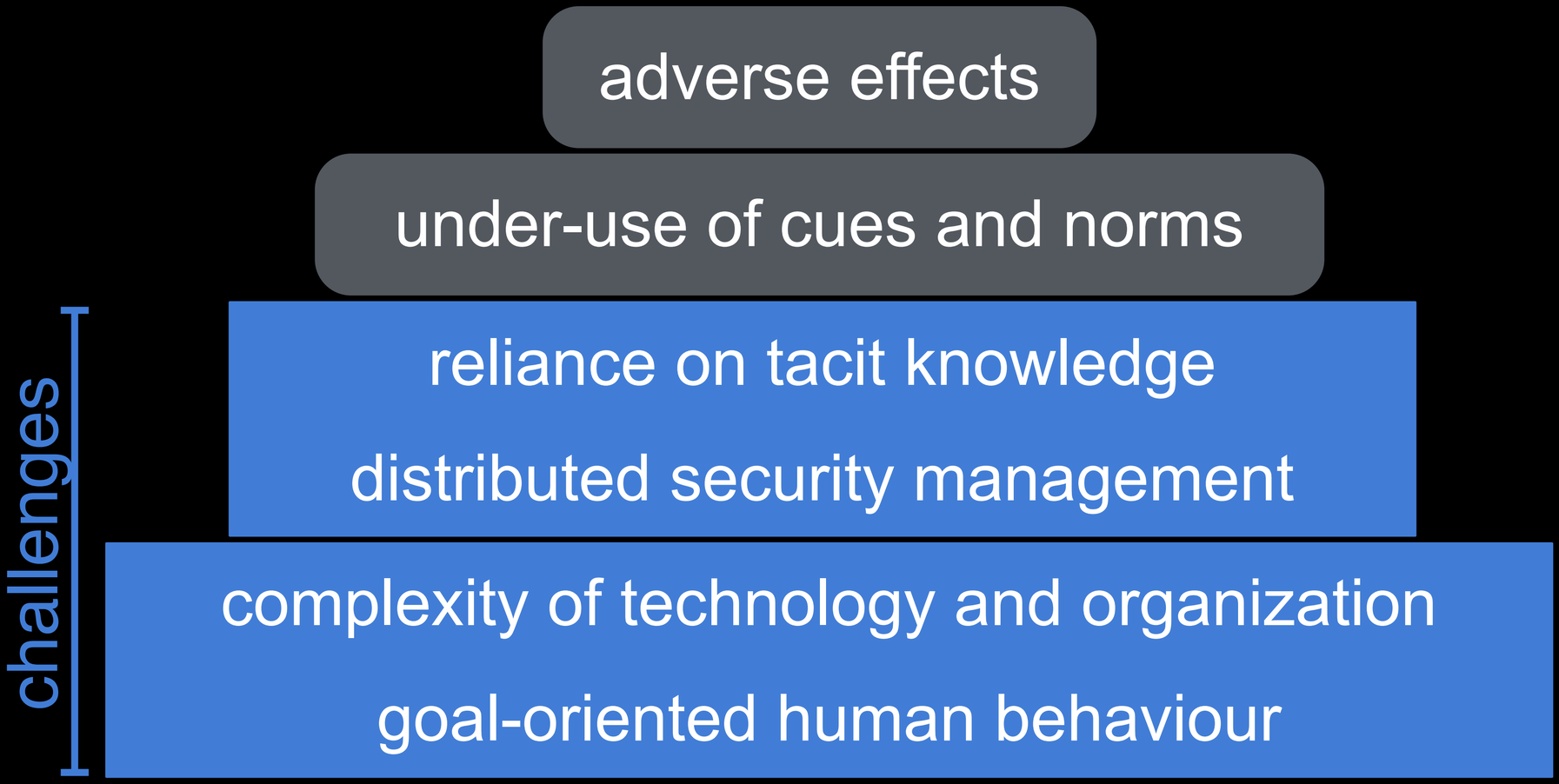
distributed cognition in ITSM: the role of cues and norms

- **cues**
  - **not explicitly directed** (e.g., quick views, proofs of reliability, and reminders & hints)
  - **explicitly directed** (e.g., scripted notifications, notes to self, and escalated notifications)

- **norms**
  - **notification procedures**
  - **methods to maintain consistency** (e.g., templates, audits, policies, and standards)
  - **establishment of mutual understanding** by means of risk assessment, promotion of security awareness, and professional collaboration
  - **employment of transactive memory** to activate the specialized knowledge and skills of others in a group

More details in:
D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, "**Toward Understanding Distributed Cognition in IT Security Management: The Role of Cues and Norms**," in the International Journal of Cognition, Technology & Work, Springer, September 2010, pp. 1-14.

distributed cognition in ITSM: challenges culminate in adverse effects



More details in:
D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, "**Toward Understanding Distributed Cognition in IT Security Management: The Role of Cues and Norms**," in the International Journal of Cognition, Technology & Work, Springer, September 2010, pp. 1-14.

guidelines for designing ITSM tools

Task Specific Guidelines

Configuration and Deployment Guidelines

Make configuration manageable [3,20]
Support rehearsal and planning [3,6,7,20,44]
Make configuration easy to change [20,46]
Provide meaningful errors [20, 34,46]

Intensive Analysis Guidelines

Provide customizable alerting [20]
Provide automatic detection [26,41]
Provide data correlation and filtering [1,26]

Organizational Complexity Guidelines

Diverse Stakeholders Guidelines

Provide flexible reporting [9,18,33,35]
Provide an appropriate UI for stakeholders [9,35]

Communication Guidelines

Provide communication integration [6,7,28,45]
Facilitate archiving [17,21]

Distributed ITSM Guidelines

Support collaboration [6,7,20]
Work in a large workflow [8,9,20]

Technological Complexity Guidelines

Make tools combinable [8,9,20,26]
Help task prioritization [15,44]
Provide customizability [9,33]
Use multiple levels of information abstraction [1,4,5,10,12,25,41,42,45]
Use different presentation / interaction methods [1,4,5,29,41,48,49]
Support knowledge sharing [9,12,14,27,32,37,47]

General Usability Guidelines

Specificity

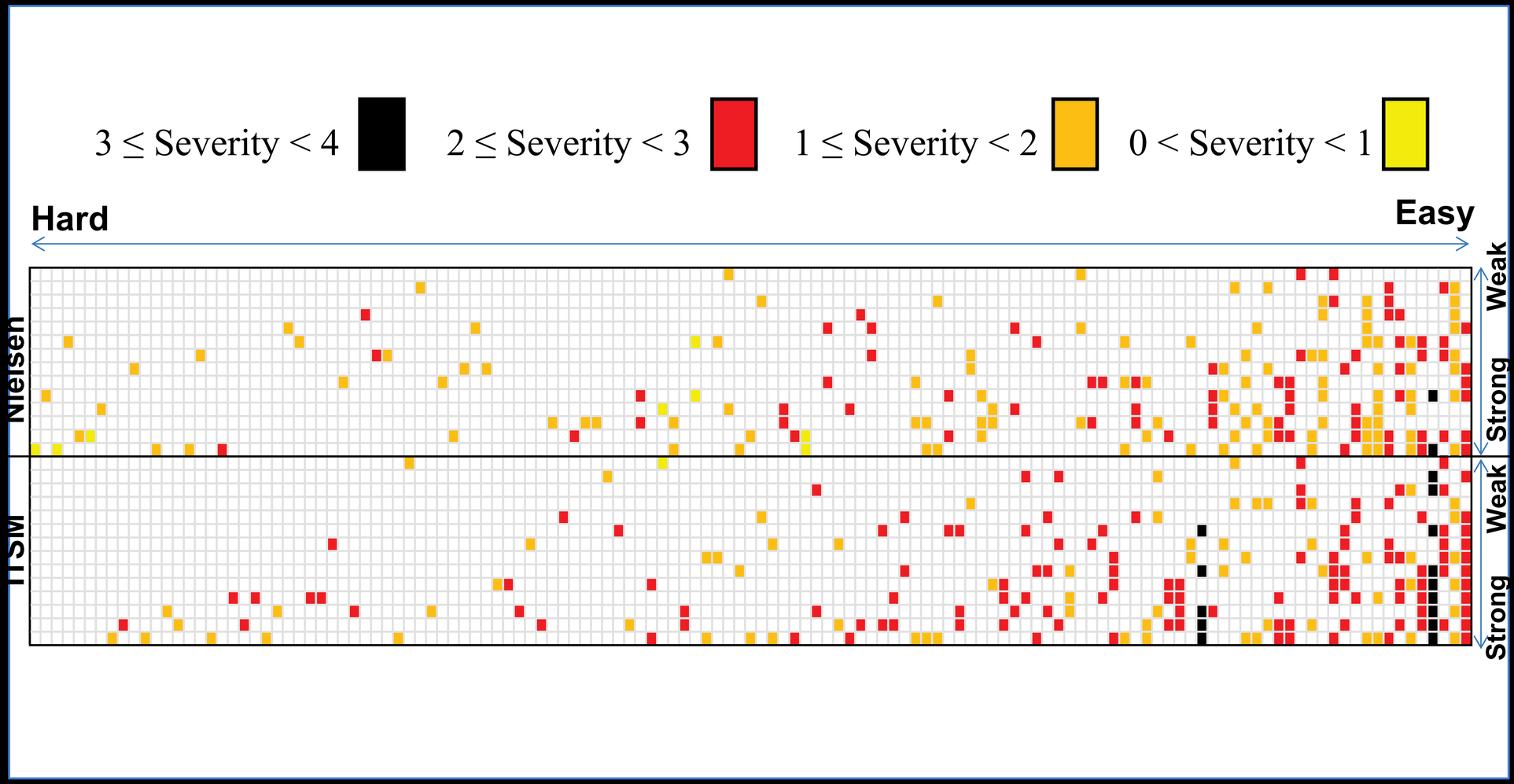
More details in:
P. Jaferian, D. Botta, F. Raja, K. Hawkey, K.Beznosov, "**Guidelines for design of IT Security Management Tools**" in ACM Computer Human Interaction for Management of Information Technology (CHIMIT) Symposium, November 2008, 10 p.

heuristics for evaluating ITSM tools

Provide Data Correlation and Filtering	Provide Automatic Detection	Provide Customizable Alerting	Provide Meaningful Errors	Make Configuration Easy to Change	Support Rehearsal and Planning	Make Configuration Manageable	Support Collaboration	Work in a Large Workflow	Provide Flexible Reporting	Provide an Appropriate UI for Stakeholders	Facilitate Archiving	Provide Communication Integration	Help Task Prioritization	Provide Customizability	Use multiple levels of information abstraction	Use different presentation/interaction methods	Support knowledge sharing	Make Tools Combinable	
							■		■			■			■	■			Visibility of activity status
						■					■								History of actions and changes on artifacts
■		■							■	■				■	■			■	Flexible representation of information
										■					■	■			Rules and constraints
							■	■					■						Planning and dividing work between users
				■		■					■						■		Capturing, sharing, and discovery of knowledge
					■	■													Verification of knowledge

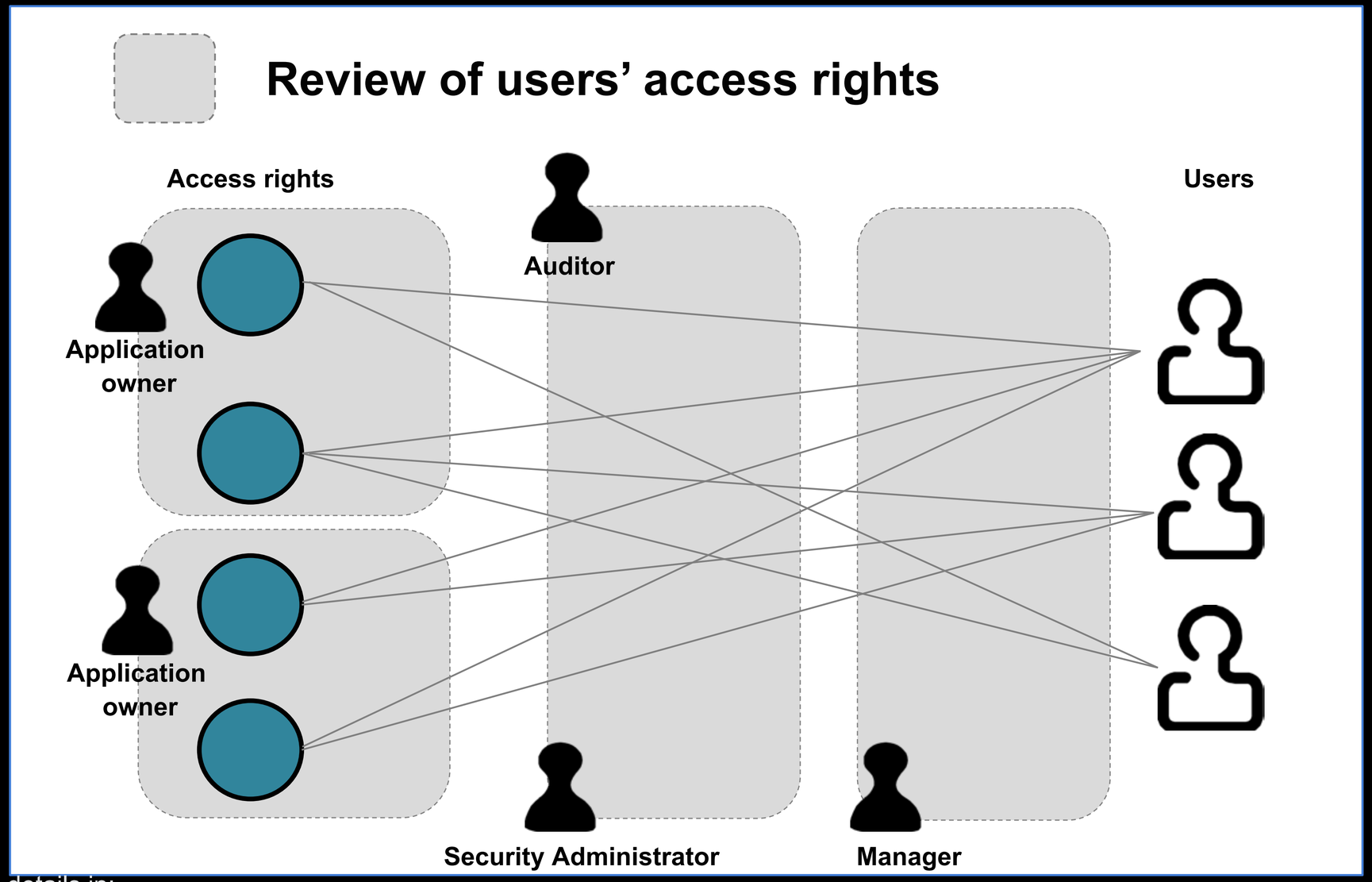
More details in:
P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, K. Beznosov, "**Heuristics for Evaluating IT Security Management Tools**," in *Human–Computer Interaction*, July 2013.

evaluating the heuristics



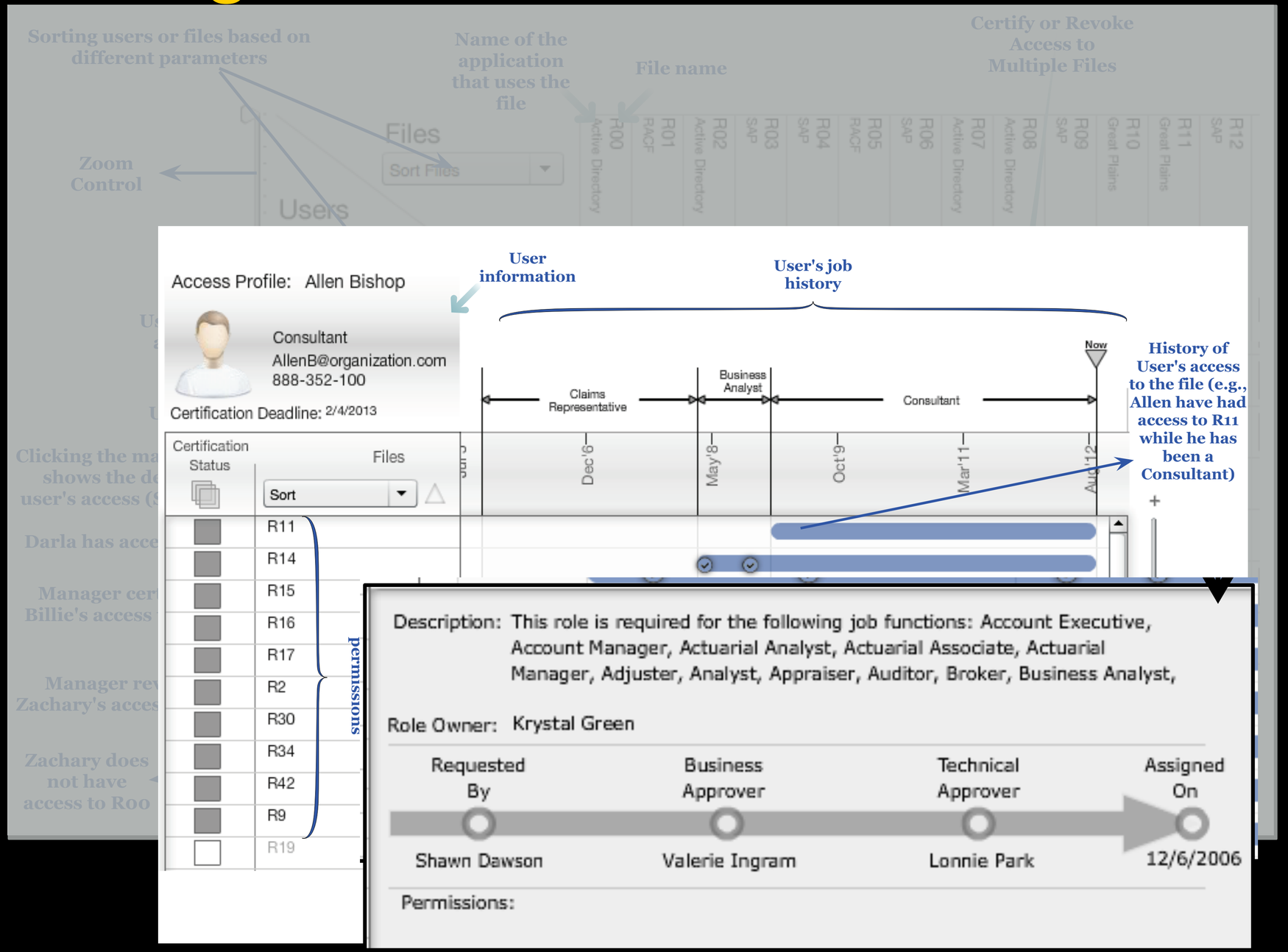
More details in:
P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, K. Beznosov, "**Heuristics for Evaluating IT Security Management Tools**," in *Human–Computer Interaction*, July 2013.

access certification



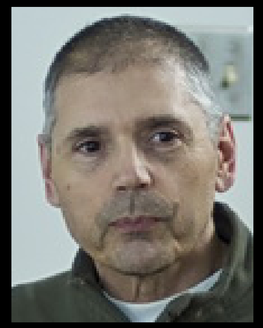
More details in:
P. Jaferian, H. Rashtian, K. Beznosov, "**To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations**," in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), USA, July 9-11, 2014, pp. 301-320.

aiding in access review and certification

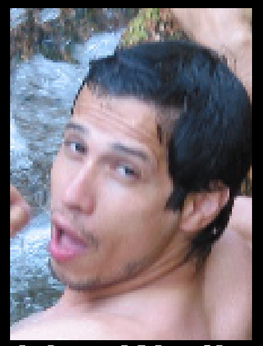


More details in:
P. Jaferian, H. Rashtian, K. Beznosov, "**To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations**," in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), USA, July 9-11, 2014, pp. 301-320.

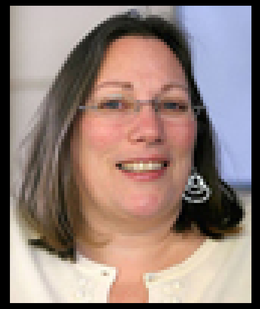
research team



David Botta



Rodrigo Werlinger



Kirstie Hawkey

Kasia Muldner

Kosta Beznosov

Sid Fels

Pooya Jaferian

Fahimeh Raja

Brian Fisher

André Gagné

selected publications

- P. Jaferian, H. Rashtian, K. Beznosov, “To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations,” in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), July 2014, pp. 301-320.
- P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, K. Beznosov, “Heuristics for Evaluating IT Security Management Tools,” in Human–Computer Interaction, July 2013.
- D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, “Toward Understanding Distributed Cognition in IT Security Management: The Role of Cues and Norms,” in the International Journal of Cognition, Technology & Work, Springer, September 2010, pp. 1-14.
- R. Werlinger, K. Muldner, K. Hawkey, K. Beznosov, “Examining Diagnostic Work Practices during Security Incident Response” in the Journal of Information Management & Computer Security, Emerald, v. 18 n. 1, 2010, pp.26 - 42.
- R. Werlinger, K. Hawkey, K. Beznosov, “An Integrated View of Human, Organizational, and Technology Challenges in IT Security Management,” in the Journal of Information Management & Computer Security, Emerald, v. 17, n. 1, January 2009, pp. 4-19.
- R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, K. Beznosov “The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?” in Proceedings of the SOUPS, Pittsburgh, PA, 23-25 July 2008.
- A. Gagné, K. Muldner, K. Beznosov, “Identifying Security Professionals' Needs: a Qualitative Analysis”, in *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.
- D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, “Towards understanding IT security professionals and their tools,” in *SOUPS*, pp. 100-111, Pittsburgh, PA, July 18-20 2007.
- 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.

Konstantin (Kosta) Beznosov

looking for new graduate students!

konstantin.beznosov.net/professional