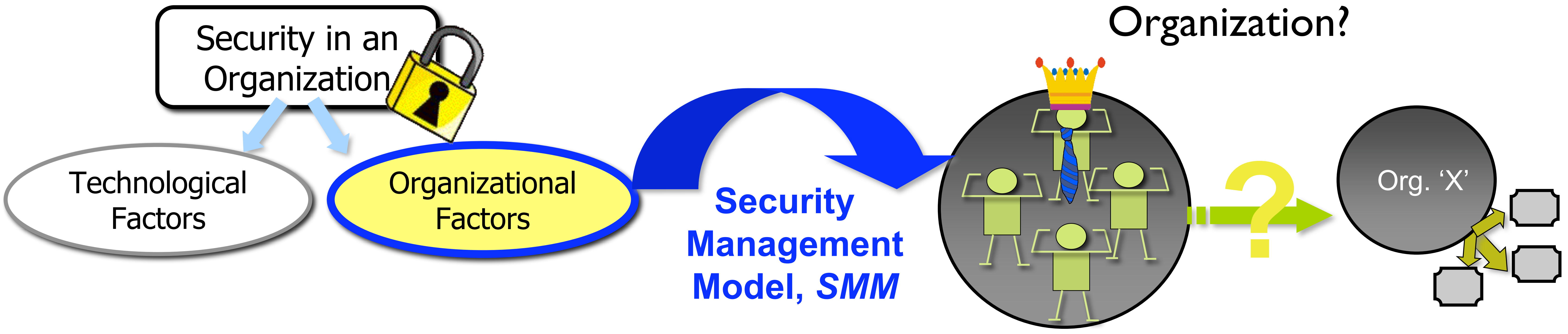
Searching for the Right Fit: Considerations when Balancing IT Security Management Model Tradeoffs

Kirstie Hawkey, Kasia Muldner and Konstantin Beznosov
Department of Electrical and Computer Engineering, University of British Columbia http://hotadmin.org

How to Position the Security Team in an Organization?



SMM Types

None : formal security team does not exist

Centralized: security team is centrally located

Decentralized: security team is interspersed throughout

Hybrid: both a centralized and decentralized component

One Organization (SLU)'s Experience

- Case study part of HOT-Admin (Human, Organizational, Technological) project

  Goal: devise support for Security Practitioners

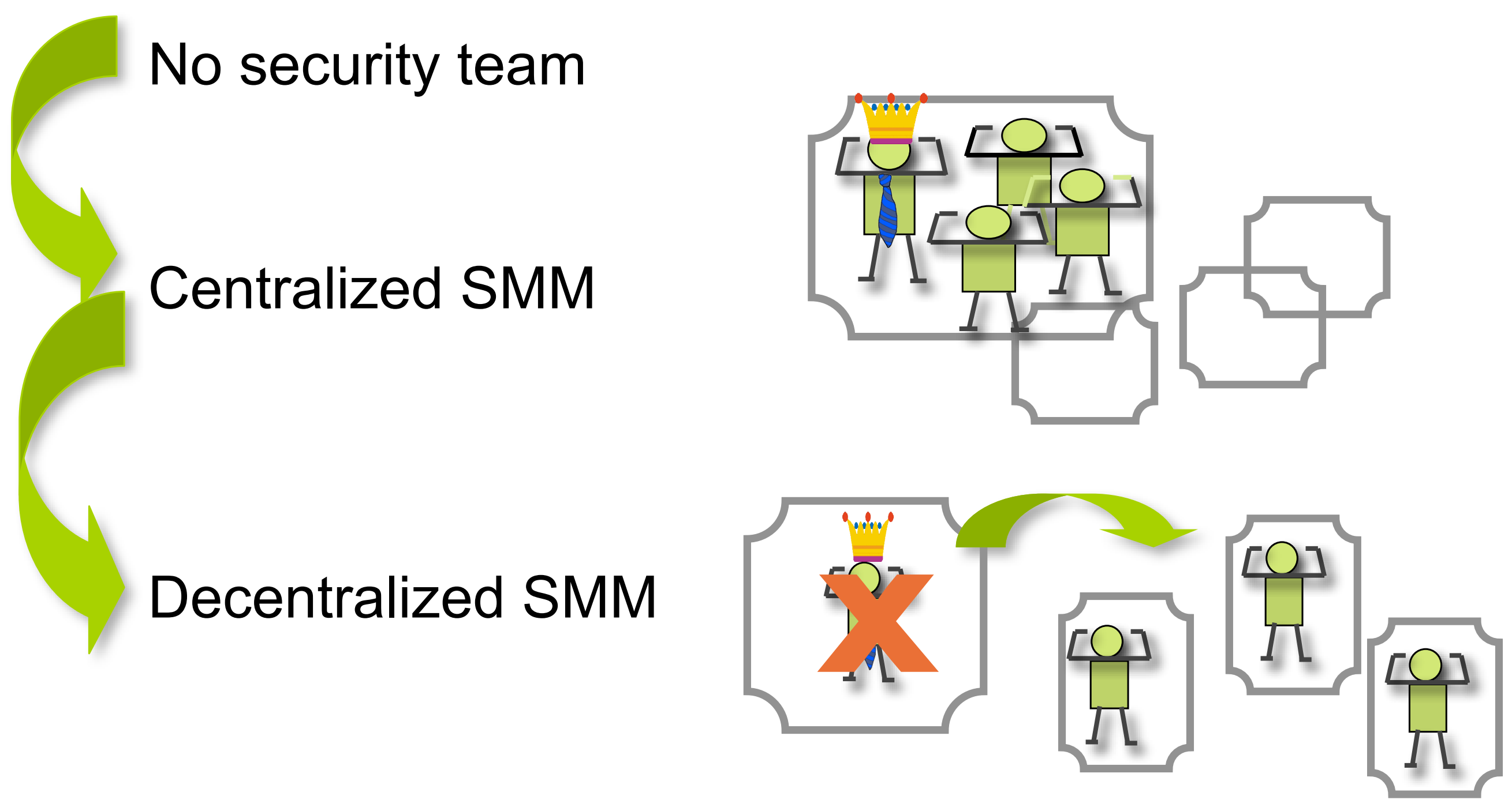
  Starting point = field study

  To date, 34 interviews with IT professionals

- Case study: 10 participants from one organization (some large university, **SLU**)

  Diverse & distributed

SLU's SMM Phases



No security team

Centralized SMM

Decentralized SMM

How did SLU's Experience Match CERT Expectations?

	None	Centralized		Decentralized		Hybrid
	CERT	CERT	SLU	CERT	SLU	CERT
Consistency	*	***	*	**	*	**
Responsiveness	*	**	**	***	**	**
Expertise	*	**	**	**	**	***
Commitment	*	***	***	**	**	***
Communication	*	***	***	*	***	**
Promotion	*	***	***	**	**	***
Buy-in	*	**	*	**	*	**
Procedures	*	***	***	**	***	***

Some Implications

Centralized SMM:

- Provided a dedicated team that promoted security in the decentralized organization
- Mismatches in expectations due to lack of authority to enforce security ➡ lack of buy-in

  Merely being informed of security does not result in stakeholders addressing security responsibilities
- Perception that security was too divorced from daily operations

Decentralized SMM:

- Mismatches with industry standards due to

  1) Lack of central manager

  2) Ability of team to function cohesively
- Surprisingly effective!

Final Thoughts

- Challenging to implement a SMM that does not completely fit with organizational attributes
- SMM need to evolve along with the organization; SMM shifts are attempts to mitigate negative organizational traits (lack of authority) as well as to reflect current organizational goals
- With each ``swing'' between SMMs, an organization may find that it is able to incorporate more and more of its prior practices, in essence moving towards a hybrid model with attributes customized to and most appropriate for the organization