

Challenge

**Social Model / Framework of Organization
to Map the Culture of Cyber Risk**

**Tom Holt, Criminal Justice
Ross Koppel, Sociology
Susan Squires, Anthropology**

Problem

Risk must be understood at the organizational/
system level to fully leverage security interventions

Goal

Capture Organizational (System Level)

- Knowledge: group level beliefs and values that shape awareness, and subsequent behaviors
- Structures including cost benefit incentives and policy interventions
- Information systems that transmit and reinforce knowledge
- Technical systems that can support appropriate technical solutions.

Organizational Knowledge

- Mission and purpose: shared values. norms of the organization, ideas about risk that informs/ influences individual behaviors
- Shared Mental Models in Work: risk perceptions, incentives, security beliefs and values
- Organizational rules about security: how workgroup enforce rules or encourage that people to break them

Associated Challenge: Design of cyber infrastructure

Organizational Structure

- Size, geographical scope, and complexity, hierarchy type
- Leadership: Effectiveness & Expertise
- Employee skills and knowledge including the tacit knowledge, or the know-how, demographics
- Employee work communities: Social dynamics, “apprenticeship” of new employees, workgroup understandings of security and support of security rules

Associated Challenge: Preserving Individual Agency in Cyberspace, Incentivization software and systems development

Information Systems

Knowledge Management and Communication

- Knowledge sharing mechanisms
- Information management policy and procedures
- Organizational methods for communicating information and ideas
- Employee communication about cyber security

Associated Challenge: Cyber crime reporting, Design of cyber infrastructure

Technical Systems

- Place and status of IT in the Organization
- Organizational value of IT: Purpose of IT, Percent of resources devoted to IT,
- Physical location of IT. Who and how are security rules enforced? Outsourced or in-house. What support does management give.
- IT's Mental Models: beliefs and values

Associated Challenge: Incentivization for software and systems development

Requirements

- Based on empirical observational data - technology, human centric, and social/organizational
- Be applicable for investigations in multiple organizations
- Establish conventions for data analysis, and modeling results so that results are reproducible
- Provides a basis for cyber-security theory building in organizations

Collaboration of multi-disciplinary teams

- Quantitative methods (technology professionals, data scientists, math/stats)
- Qualitative methods (disciplines that study individuals and social groups)
- Create a common set principles about what is rigorous and publishable
- Principles must be understood from different perspective as well as from one that is shared