Risk Perception in IT Security

Mary Ellen Zurko

mez@alum.mit.edu

What is the perception of risk for IT workers?

- Different roles and positions view and accept risk differently
  - Operators
  - Administrators
  - Security Officer
  - IT Management
  - Management chain

- Citable SOUPS research is on IT security management and protection

Actions Taken For Security Purposes

- Patching
- Monitoring (security)
- Testing
- Deploying (security)
- Configuration checking
- Auditing (in the compliance sense)

- Actions taken for other purposes can affect security
  - Zero risk perception?

Compliance – Familiar Lens for Risk

- Adhere to established (and iterating) best practices for the business, its vertical, its geography(s), including appropriate legal regulation
- Each (large) company has its own
- Rules, requirements, processes
- Changes require modifications
  - Must be written so it can be broadly used
  - Must be written so risk can be tolerated by the business
- “If I am in compliance, my risk is covered”
  - “Am I in compliance?”

Risk of IT Not Covered by Compliance?

- What happens when part of your IT is not under your specific Compliance regime?
  - Cloud
- How do you perceive (and mitigate) risk in those areas?
  - Legal contract
  - Public documentation
  - Visibility into externally contracted IT
- What do you look for?
  - Alignment with your existing compliance
    - Real or analogous
  - Legal and financial ownership of (perceived) risk
- Risk is perceived in business terms
  - Legal, financial, position, job, politics

Are Humans Increasing Our Risk?

- Are Humans Risk Generators?
- Are they subverting compliance?
- Is it worth finding out?
- Is it worth doing something about?
- Can we argue that they're not?
- Will burdensome security decisions reduce our risk as we perceive it?

What Could Risk Perception of IT Ops Be Based On?

- What information do they get, and what should they get?
  - Risk perception in a vacuum?
- What is their risk of changing or setting a configuration and getting it wrong?
- What is the risk of the current state? If it is in compliance, out of compliance, not covered by compliance?
- What is the risk of the specific change history?
  - People involved?
  - Times of changes?

Are We Under Attack?

- Risk perception includes threat perception
- Are we under attack?
- Is that any different from anyone else?
  - What does the press say about it?
- Are our defenses any better or worse than anyone else?
- Has any of that changed?
- Are we (more) attractive as a target?
- Is it better not to know?

Individuals' Risk Perception within their Organization

- Research on individual risk perception in isolation does not take account of organizational structures for managing and mitigating risk
  - Risk perception must be different within organizational contexts
  - For all the reasons above

- Thank you

mez@alum.mit.edu