An estimated 90% of cybersecurity breaches worldwide occur in small businesses. 75% of SMBs could not continue operating if they were hit with ransomware. 82% of ransomware attacks in 2021 were against companies with <1,000 employees.

**Problem: SMEs struggle to balance productivity and operational efficiency against cybersecurity**

- An estimated 90% of cybersecurity breaches worldwide occur in small businesses
- 75% of SMBs could not continue operating if they were hit with ransomware
- 82% of ransomware attacks in 2021 were against companies with <1,000 employees

**Purpose: Develop a Cybersecurity Culture Model to be Transmitted Across Organizations**

1. **Quantify cybersecurity culture mismatch** between large companies and their suppliers to understand the impact on working relationships
2. **Identify mechanisms** required to align cybersecurity culture across companies
3. **Determine interventions and leading practices** that will help address culture mismatch
4. **Highlight how cybersecurity culture can be propagated** to suppliers

**Research Process: What We Are Doing (2-Step Process)**

1. **Survey** to assess the culture of the large company and a supplier
   - Results will map the two cultures based on each org’s values, attitudes, and beliefs around cybersecurity and quantify culture mismatch
2. **Interviews and fieldwork** to measure cultures in action
   - Characterize the relationship between large companies and suppliers (e.g., types of interactions, frequency, information exchanged, etc.)
   - Understand mechanisms underlying relationships (e.g., organizational barriers, drivers for change, internal development efforts, etc.)

**How to Measure Culture (Huang and Pearlson, 2019)**

**External Influences**
- Societal/National Cybersecurity Culture
- External Rules and Regulations
- Peer Institutions

**Managerial Mechanisms**
- Culture Leadership
- Communications Plan
- Performance Evaluation
- Rewards and Punishments
- Cybersecurity Training
- Organizational Learning

**Culture: Beliefs, Values, and Attitudes**

- **Leadership Level**
  - Top Management Priority
  - Top Management Participation
  - Top Management Knowledge

- **Group Level**
  - Community Norms and Beliefs
  - Teamwork
  - Inter-Department Collaboration

- **Individual Level**
  - Employee Self-Efficacy
  - Cybersecurity Policy Awareness
  - General Cyber Threat Awareness

**Behaviors**
- Job-related Cybersecurity Behavior
- Organ-related Cybersecurity Behavior

**Get Involved: Be Part of A Case Study!**

- We are looking for 5-6 case studies with organizations who have existing programs to help their SMEs with their cybersecurity
- Our goal is to highlight leading practices to improve SME cybersecurity in the supply chain
- Interested? Or know an organization that fits? Contact Dr. Jillian Kwong, jkwong1@mit.edu

Research funded in part by a grant from the HPI-MIT Designing for Sustainability Program. For more information, scan the QR code.