Misalignment and Mismatch: Cybersecurity Complexities of Small to Medium-Sized Enterprises (SMEs) in the Supply Chain

Identifying Areas of Complexity Impeding SME's ability to be cybersecure

Dr. Jillian Kwong | jkwong1@mit.edu
Dr. Keri Pearlson | kerip@mit.edu

October 2023

Problem: SMEs cannot meet minimum security standards required by supply chain partners

Compromised supply chains have become a major risk to businesses around the world causing significant disruption to global supply chains. Small and medium-sized enterprises (SMEs) are particularly vulnerable struggling with shortages in staffing, funding, knowledge, detection, response, and recovery

- **~75% of SMEs could not continue operating if hit with ransomware**
- **46% of all cyber breaches impact businesses with <1,000 employees**
- **43% of SMEs lack any type of cybersecurity defense plan**

Study Goals: Help SMEs Become Better Supply Chain Partners

✓ Identify areas of complexity that have impeded SMEs' ability to be cybersecure partners in supply chains

✓ Develop leading practices and recommendations to improve SME cybersecurity capabilities and promote cooperative relationships between buyers and suppliers.

RQ's

RQ_1: What challenges have SMEs encountered implementing cyber mandates into organizations?

RQ_2: What are SMEs and large organizations doing to address these challenges?

Actionable Insights: Regulators, SMEs, and Large Companies

- **Regulators need to design legislation with SMEs and their resource capabilities in mind**
- Large companies need to develop programs to set expectations and help match their culture of cybersecurity with SMEs
- **SMEs must ask large companies for help aligning frameworks**
- Bring cybersecurity discussions earlier in procurement process

Findings: Cybersecurity Environment too Complex for SMEs

UNFRIENDLY REGULATION

Cybersecurity regulations lack tangible penalties to motivate action or organizational change. Unlike the data privacy focused regulations such as the General Data Protection Regulation (GDPR), the lack of tangible penalties in cybersecurity legislation makes it difficult to prioritize and advocate for additional cybersecurity resources internally.

Many SMEs who supply or work with larger companies are indirectly subject to legislation and did not have the knowledge or expertise to decipher how regulations apply to their organization

ORGANIZATIONAL CULTURE CLASHES

SMEs struggled to balance operational efficiency and productivity demands with cybersecurity requirements lacking the organizational culture to support both at once

FRAMEWORK VARIABILITY

When large companies develop their own approaches to cybersecurity and GRC, they decide which standards (e.g., NIST Cybersecurity Framework, ISO 27000+, etc.) to orient processes around. However, this creates a burden for SMEs who supply to more than one customer and subsequently struggle to comply with the nuances of multiple standards at once

Get Involved: Be Part of A Case Study!

- We are looking for **5-6 case studies with organizations who have existing programs to help SMEs with their cybersecurity**
- Our goal is to study how orgs develop, align, and transmit shared values, attitudes, beliefs, and practices across the supply chain
- Interested? Or know an organization that fits? Contact Jillian Kwong, jkwong1@mit.edu