Exploring Shortcomings in Third Party Risk Management of Small and Medium-Sized Enterprises (SMEs)

How and why traditional methods fail to improve third party risk assessments of SMEs

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

Cybersecurity at MIT Sloan

Problem: SMEs Struggle with Cybersecurity

Small and medium-sized enterprises (SMEs) have long been known to be a weak link in supply chain cybersecurity. Despite their crucial role in the global supply chain, SMEs and their struggle to increase cyber resiliency and improve their defenses is understudied in academic literature.

Reason 1: As large companies shore up cybersecurity defenses, SMEs become more attractive targets for attackers to breach systems
Reason 2: Major frameworks to reduce risk and improve cybersecurity are not designed for SMEs
Reason 3: SMEs are understudied in academia, industry, and government

What Cybersecurity Challenges do SMEs Encounter when Participating in Third Party Risk Assessments?

- A qualitative approach was used to conduct an empirical study of the challenges SMEs encounter when participating in third party risk assessments. Results discuss how and why traditional methods fail and offers insights on how to improve third party risk assessments of SMEs moving forward.

How We Did It: Semi-Structured Interviews

- Semi-structured interviews with SME security specialists, supply chain managers, legal and compliance experts, business leadership
- Data analyzed using two-cycle coding

Actionable Insights for Realigning Processes

- Align processes to standards
- Determine efficacy of new tools and processes
- Utilize existing resources offered by organizations to streamline processes
- Cybersecurity risk is business risk

Shortcomings of Traditional Risk Assessment Methods When Applied to SMEs

Types of Assessment Tools	Strengths	Weaknesses
Questionnaires and Surveys (e.g., based on ISO 27000+)	• Cheap • Easy to administer • Widely used and accepted throughout the industry	• Based on self-report/self-attestation • Long, time consuming (1000+ questions), and low response rates • Only as good as respondent is honest • Often too vague to be actionable or useable
Audits and Certifications (e.g., System and Organization Controls (SOC) 2 reports)	• Establishes standards to benchmark security against • Provides documentation • Signals leadership has begun to think about/invest in security	• Reflects security on the day the organization was audited or certified • Expensive and time consuming • Only as good as the person auditing/certifying • Criticized as “Pay to play” system
Security Rating Services (e.g., BitSight, SecurityScorecard, RiskRecon, etc.)	• Offers an “objective” (i.e., not a self-assessment) rating of an organization’s security	• Only depicts one aspect of an organization’s security • Criticized as “Pay to play” system
Direct Testing (e.g., penetration testing and red team assessments)	• One of the most reliable ways of assessing 3rd party security	• Cost • Time consuming • Liability • Permissions

October 2023