Supplier Development Framework in Supply Chain Cybersecurity Evaluation of Small and Medium-sized Enterprises (SMEs)

Building a supplier development framework for improved mutual capability building

Alex Chang (ecalex@mit.edu), Dr. Jillian Kwong (jkwong1@mit.edu), Dr. Keri Pearlson (kerip@mit.edu)

Cybersecurity at MIT Sloan

Cyber Risk in Supply Chain

- Supply chain (SC) cybersecurity are more crucial as corporations integrate suppliers into their systems and SC.
- About 40% of data security breaches arise from attacks on suppliers (Melnyk, 2022). Despite this, vendor oversight in cybersecurity is one area that lacks in-depth investigation.
- There is a lack of cyber capability development between supplier assessment and subsequent collaboration.

Developing Supplier Capability

- The supplier development process intends to provide a guideline for procurement, cybersecurity, and risk management professionals to assess and develop software, hardware, and service suppliers on an ad-hoc and regular basis. The framework serves to augment business processes with the best practices in SC management.
- Defines persona using this process as a larger purchasing organization (client) working with its SME suppliers.
- Process runs independently of other processes, focusing on supplier development in cybersecurity capabilities.
- The framework assumes the client, because of sourcing needs, is considering and qualifying suppliers for an approved vendors list (AVL) consisting of both larger and smaller suppliers.

Building a Security-Centric Sourcing Strategy Through Supplier Development

- Review and implement vendor-specific requirements.
- Widen potential supplier pool with supplier development process.
- Work with suppliers on mutual capability building to increase value delivered.
- Iterate and improve on current supplier capabilities to decrease risk.