Securing the Global Supply Chain:

Addressing Risks Small and Medium-sized Enterprises (SMEs) Pose to Cybersecurity Supply Chains

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

Cybersecurity at MIT Sloan

Background: Compromised Supply Chains

- Compromised supply chains are a major business risk threatening information assets and disrupting everyday operations
- 742%: The average annual increase in software supply chain attacks since 2019
- $4.46 million: The average cost of a supply chain compromise
- Supply chain cybersecurity is especially difficult for small and medium-sized enterprises (SMEs)

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

Studies have found:

- 43% of SMEs lack any type of cybersecurity defense plan
- 51% have no cybersecurity measures in place
- 63% of SMEs reported experiencing a data breach within the last year

SMEs are key to supply chains, yet often lack resources for cybersecurity like larger firms.

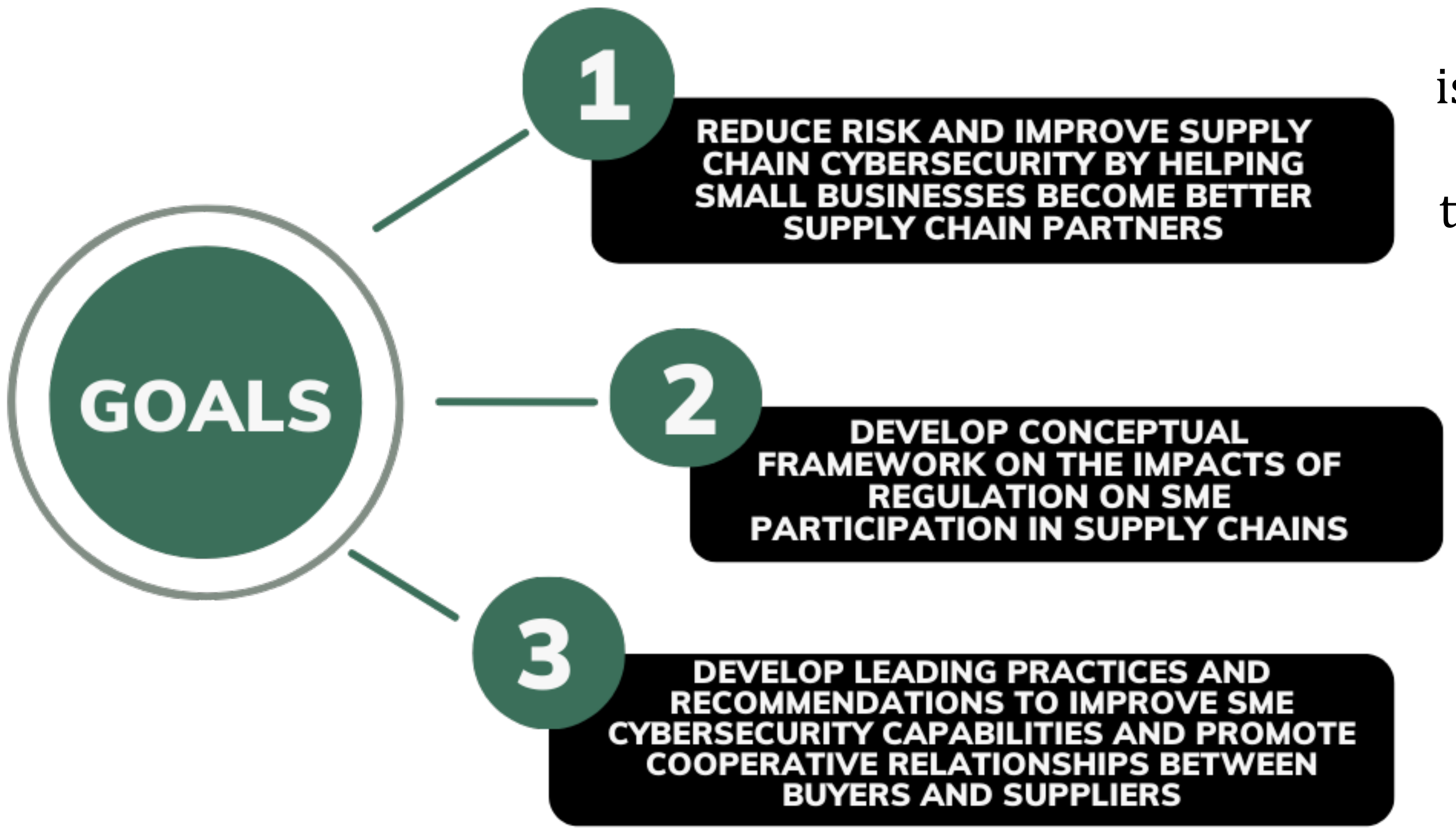
This can cause significant disruption to global supply chains as approximately 75% of SMEs could not continue operating if hit with ransomware.

Inadequate Government Response

Research has found certain regulations can destabilize supply chains by introducing greater levels of risk when SMEs leave the supply chain altogether (e.g., 2016 DoD DFARS 252.204-7012 mandate)

Study Rationale and Goals: Help SMEs Become Better Supply Chain Partners

Existing cybersecurity models and frameworks say *what* needs to be done but not *how.* Part of the problem is a lack of tools or mechanisms to enable supplier development. We believe creating a solution involves working with larger companies to understand how bigger players in the supply chain can help develop, support, and drive change in SME cyber capabilities.



1. REDUCE RISK AND IMPROVE SUPPLY CHAIN CYBERSECURITY BY HELPING SMALL BUSINESSES BECOME BETTER SUPPLY CHAIN PARTNERS
2. DEVELOP CONCEPTUAL FRAMEWORK ON THE IMPACTS OF REGULATION ON SME PARTICIPATION IN SUPPLY CHAINS
3. DEVELOP LEADING PRACTICES AND RECOMMENDATIONS TO IMPROVE SME CYBERSECURITY CAPABILITIES AND PROMOTE COOPERATIVE RELATIONSHIPS BETWEEN BUYERS AND SUPPLIERS

The first step in this process is interviewing cybersecurity and supply chain personnel to document and understand how these organizations are managing competing cybersecurity requirements and pressures.

Results of the research will provide vital insights for SMEs, regulators, and larger organizations in terms of how to best support and drive change within SMEs.

Interested? Get Involved!

Sample Questions

- What are the major cybersecurity standards, regulations, or mandates your organization complies with?
- What aspect of these rules are most difficult for your company to put in practice? Why?
- If given additional resources to help with supply chain cybersecurity where or how would you deploy them?

Support This Research

- Participate in a research interview or join a case study to help improve supply chain cybersecurity and help SMEs become better supply chain partners
- Contact **Dr. Jillian Kwong (jkwong1@mit.edu)** for more information or to participate