Supply Chain Cybersecurity for Small and Medium Enterprise

Building an evaluation framework in cybersecurity engagement between small and medium enterprises (SMEs) and corporations in supply chain

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

Weaknesses in Supply Chains

Objectives:

- Reduce risk and improve security across the supply chain
- Document current practices and issues companies face when working with 3rd parties
- Develop a framework to help SMEs prepare to be better partners/suppliers

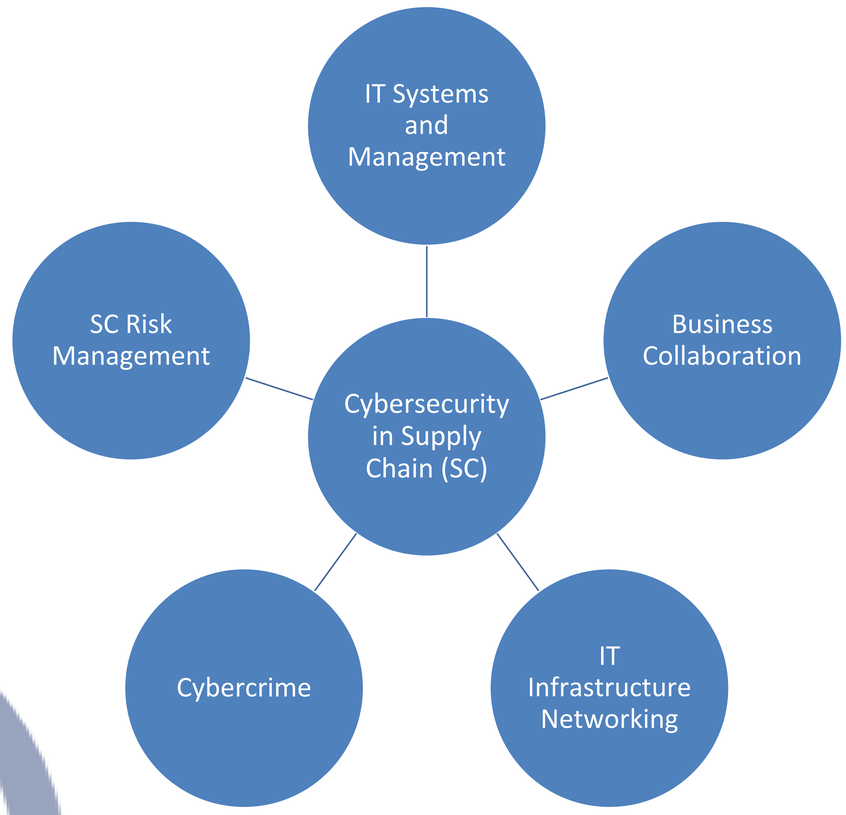
Research Questions

- What and where are the cybersecurity weaknesses in a supply chain context?
- How do companies currently evaluate the security of SME partners/suppliers? What strategies do companies use to manage or mitigate risk from 3rd parties? What issues or limitations have yet to be addressed?
- What factors decrease willingness to engage and improve cybersecurity readiness for SMEs in the supply chain?

3rd Party Risk In the Cybersecurity Supply Chain

Background Literature:

- Supply chain cybersecurity and information management has become increasingly important as corporations integrate suppliers/vendors into their systems and supply chains
- In vendor selection, more than 73% of respondents believed a vendor's cybersecurity approach influenced the respondent's willingness to engage in business with them [2]
- About 40% of data security breaches arise from attacks on corporation's suppliers [1]. Despite this, vendor oversight in terms of cybersecurity readiness is one area that lacks in-depth investigation
- Small and medium enterprises (SMEs) make up more than 97% of total businesses in North America and data breaches and cyber attacks against SMEs are on the rise [2]
- Lack of resources, expertise, and understanding are usually cited as contributing factors that hinders SME cybersecurity efforts [1-3]



Methodology

- Literature Review
- Framework and Hypotheses Development
- Interviews

References

1. Melnyk, et al. (2022) "New challenges in supply chain management: cybersecurity across the supply chain," International Journal of Production Research, 60:1, 162-183, DOI: 10.1080/00207543.2021.1984606
2. Better Business Bureau. (2017), "2017 state of cybersecurity among small businesses in North America." Available at https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf
3. Benz and Chatterjee (2020), "Calculated risk? A cybersecurity evaluation tool for SMEs", Business Horizons Volume 63, Issue 4, July–August 2020, Pages 531-540

Get Involved!

Does your company have a vendor risk management program? Would you like to help develop better strategies to evaluate 3rd party security?

Be apart of this research by **participating in an interview** or **joining a case study** to help us understand how companies are currently managing/mitigating risk from 3rd party vendors and how this process can be improved.

Stay up to date and join the research! Contact **Alex Chang (ecalex@mit.edu)** and **Dr. Jillian Kwong (jkwong1@mit.edu)** for more details.