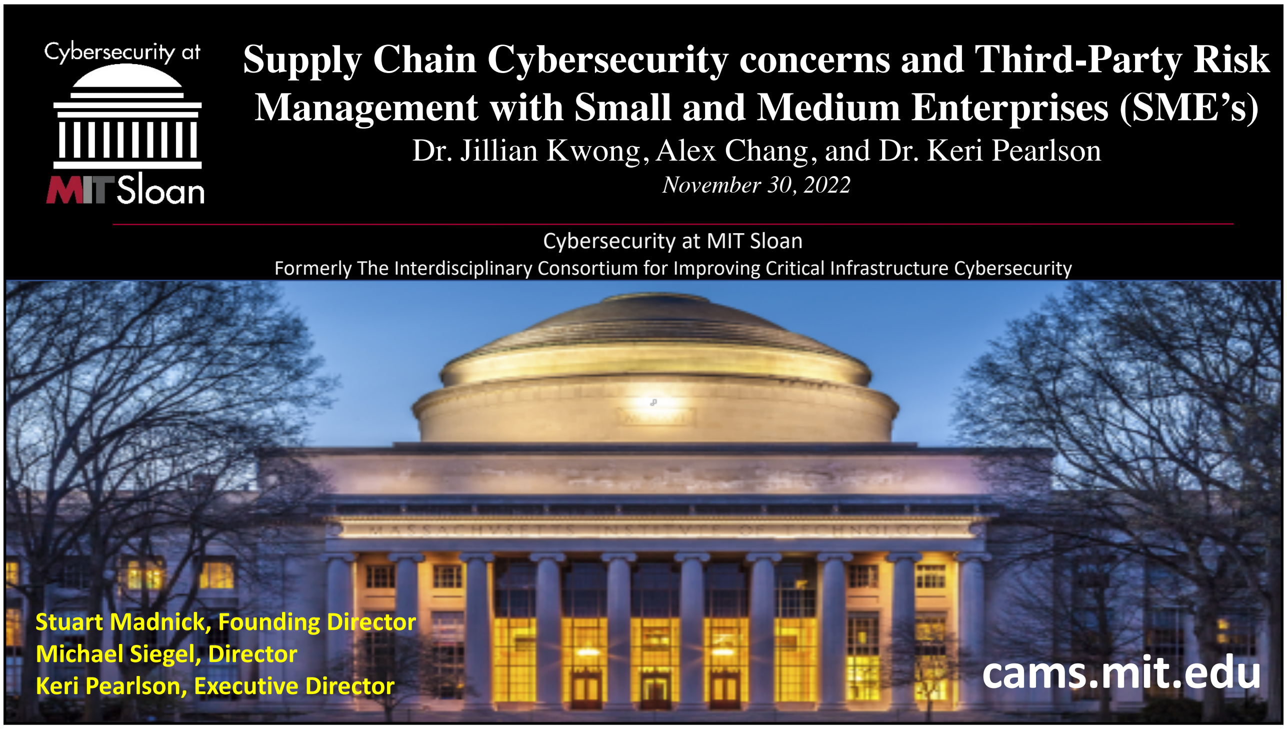


Supply Chain Cybersecurity concerns and Third-Party Risk Management with Small and Medium Enterprises (SME's)

Dr. Jillian Kwong, Alex Chang, and Dr. Keri Pearlson

November 30, 2022

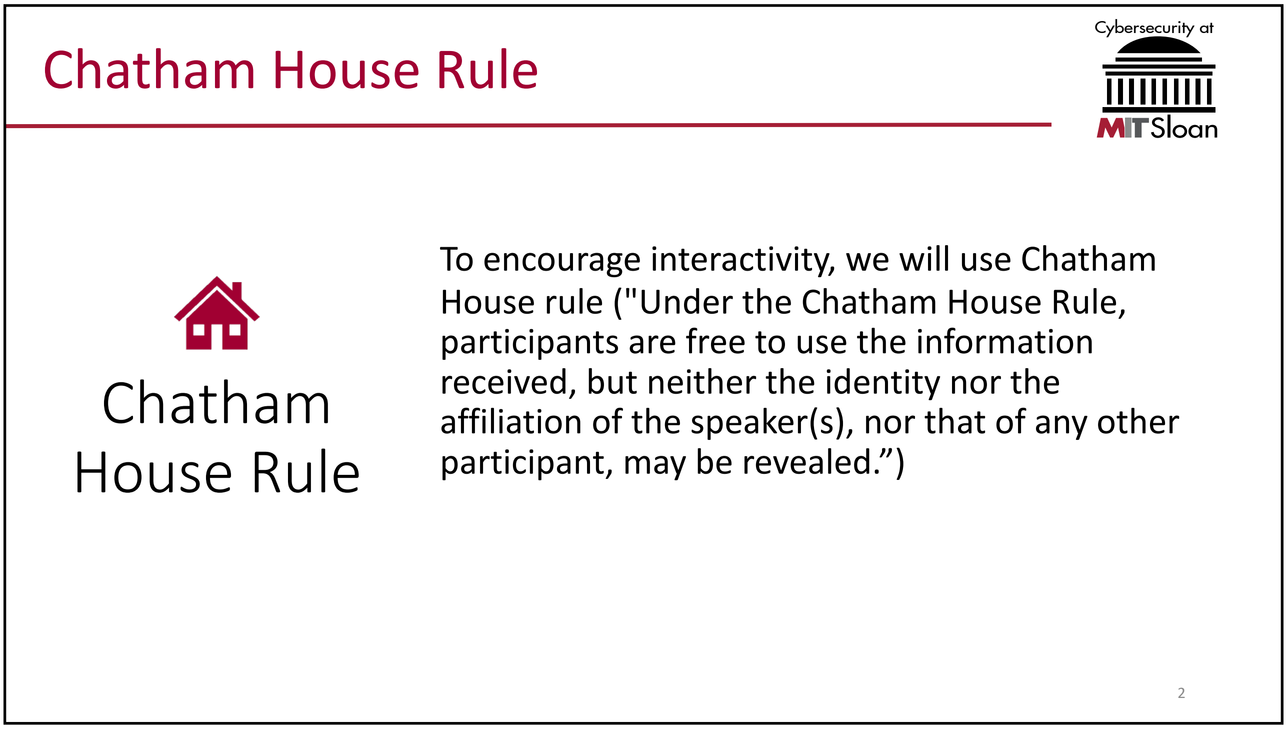
Cybersecurity at MIT Sloan

Formerly The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

Stuart Madnick, Founding Director
Michael Siegel, Director
Keri Pearlson, Executive Director

cams.mit.edu

1



Chatham House Rule

Chatham House Rule

To encourage interactivity, we will use Chatham House rule ("Under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.")

2

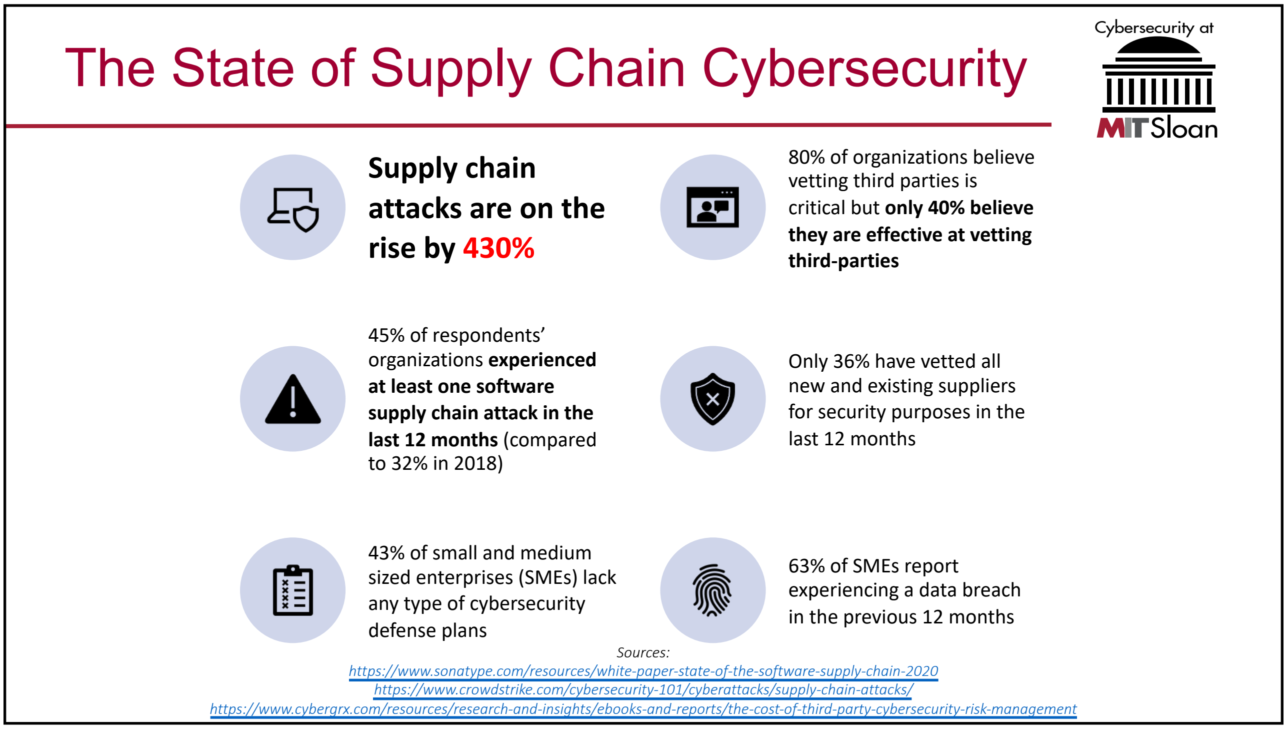
2

Supply Chain Cybersecurity

What’s on your mind?

3

3



The State of Supply Chain Cybersecurity

Cybersecurity at MIT Sloan

Supply chain attacks are on the rise by 430%

80% of organizations believe vetting third parties is critical but **only 40% believe they are effective at vetting third-parties**

45% of respondents’ organizations **experienced at least one software supply chain attack in the last 12 months** (compared to 32% in 2018)

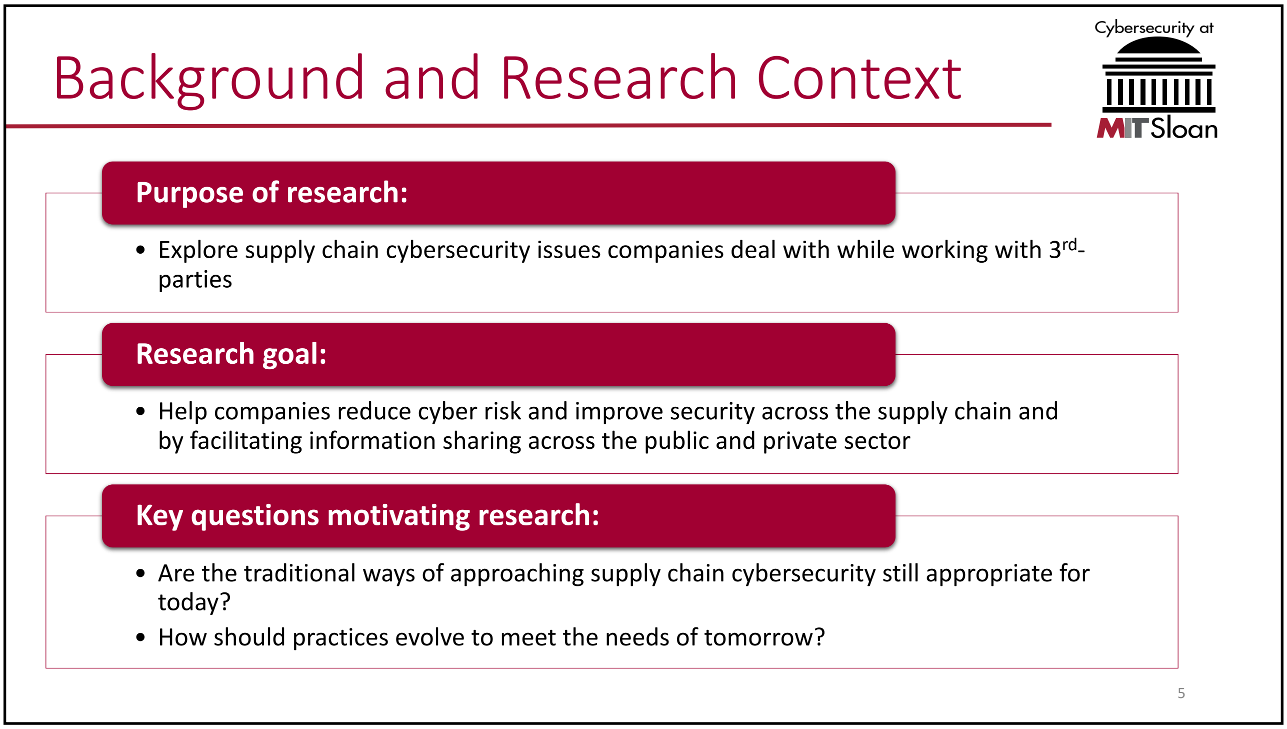
Only 36% have vetted all new and existing suppliers for security purposes in the last 12 months

43% of small and medium sized enterprises (SMEs) lack any type of cybersecurity defense plans

63% of SMEs report experiencing a data breach in the previous 12 months

Sources:
https://www.sonatype.com/resources/white-paper-state-of-the-software-supply-chain-2020
https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
https://www.cybergrx.com/resources/research-and-insights/ebooks-and-reports/the-cost-of-third-party-cybersecurity-risk-management

4



Background and Research Context

Cybersecurity at MIT Sloan

Purpose of research:

- Explore supply chain cybersecurity issues companies deal with while working with 3rd-parties

Research goal:

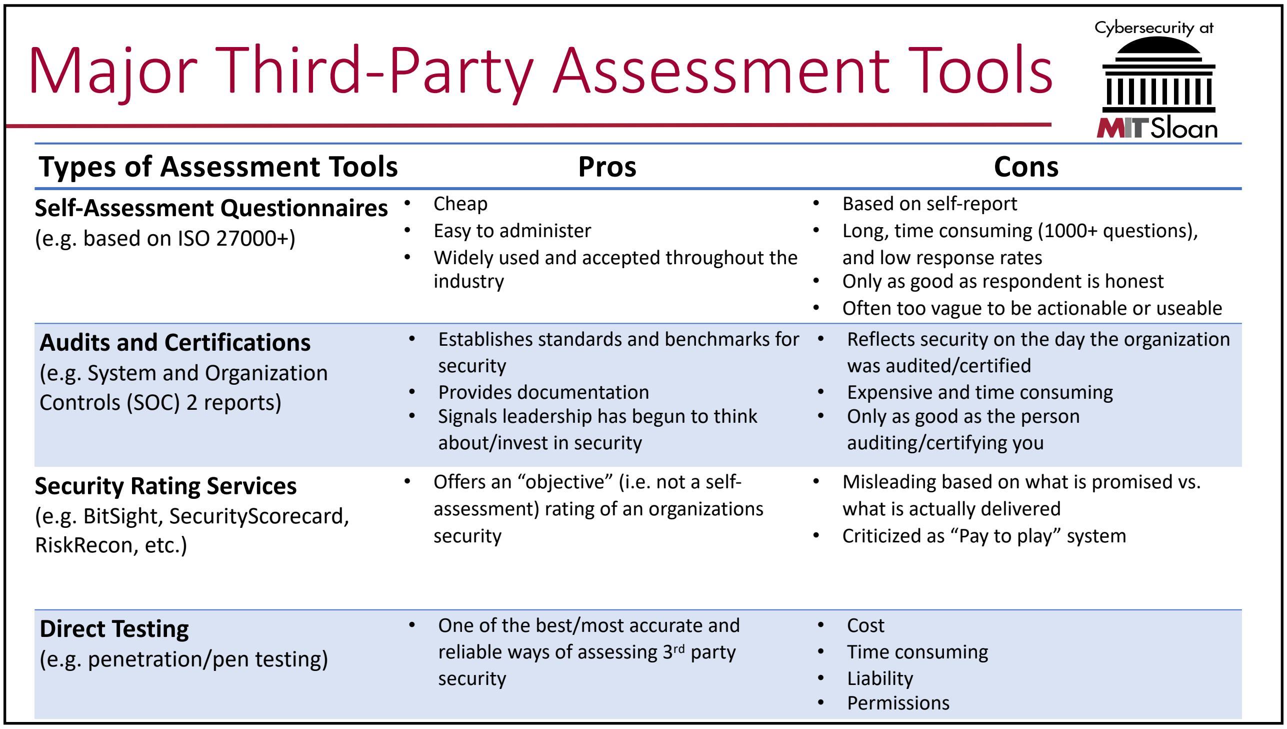
- Help companies reduce cyber risk and improve security across the supply chain and by facilitating information sharing across the public and private sector

Key questions motivating research:

- Are the traditional ways of approaching supply chain cybersecurity still appropriate for today?
- How should practices evolve to meet the needs of tomorrow?

5

5

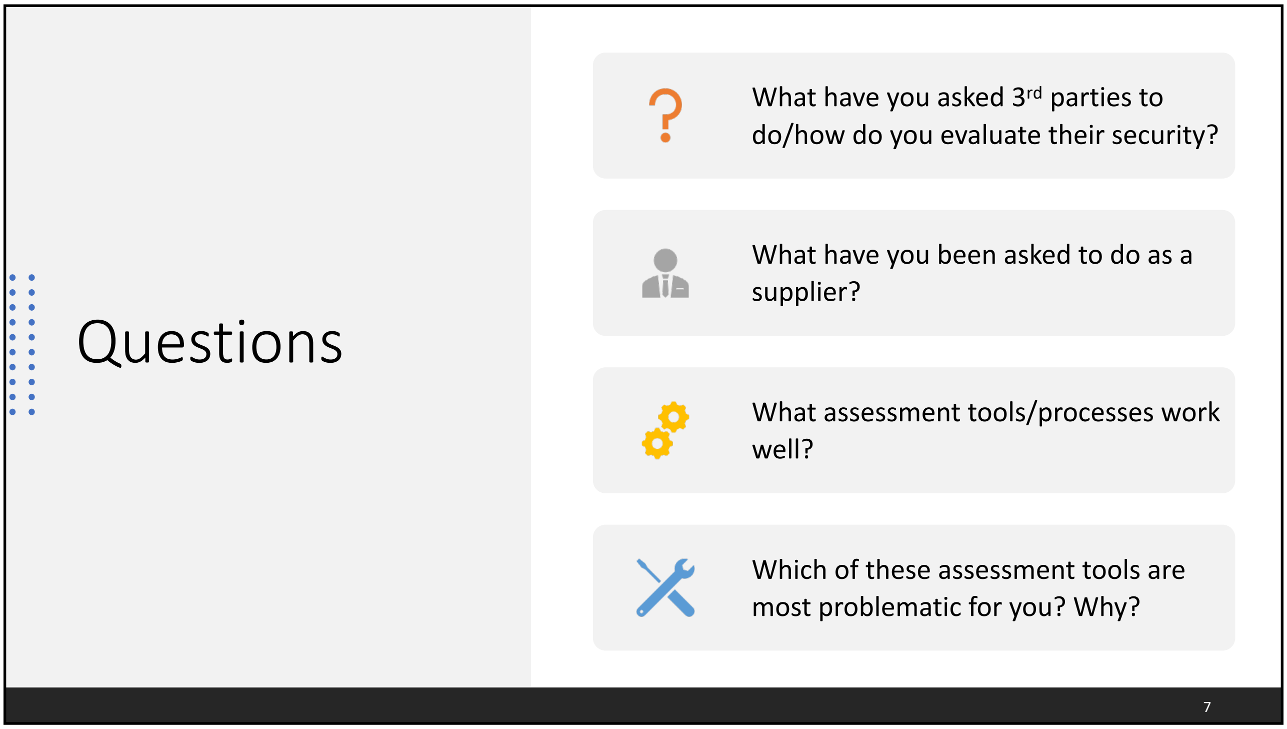


Major Third-Party Assessment Tools

Cybersecurity at MIT Sloan

Types of Assessment Tools	Pros	Cons
Self-Assessment Questionnaires (e.g. based on ISO 27000+)	• Cheap • Easy to administer • Widely used and accepted throughout the industry	• Based on self-report • 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 and benchmarks for security • Provides documentation • Signals leadership has begun to think about/invest in security	• Reflects security on the day the organization was audited/certified • Expensive and time consuming • Only as good as the person auditing/certifying you
Security Rating Services (e.g. BitSight, SecurityScorecard, RiskRecon, etc.)	• Offers an "objective" (i.e. not a self-assessment) rating of an organizations security	• Misleading based on what is promised vs. what is actually delivered • Criticized as "Pay to play" system
Direct Testing (e.g. penetration/pen testing)	• One of the best/most accurate and reliable ways of assessing 3rd party security	• Cost • Time consuming • Liability • Permissions

6

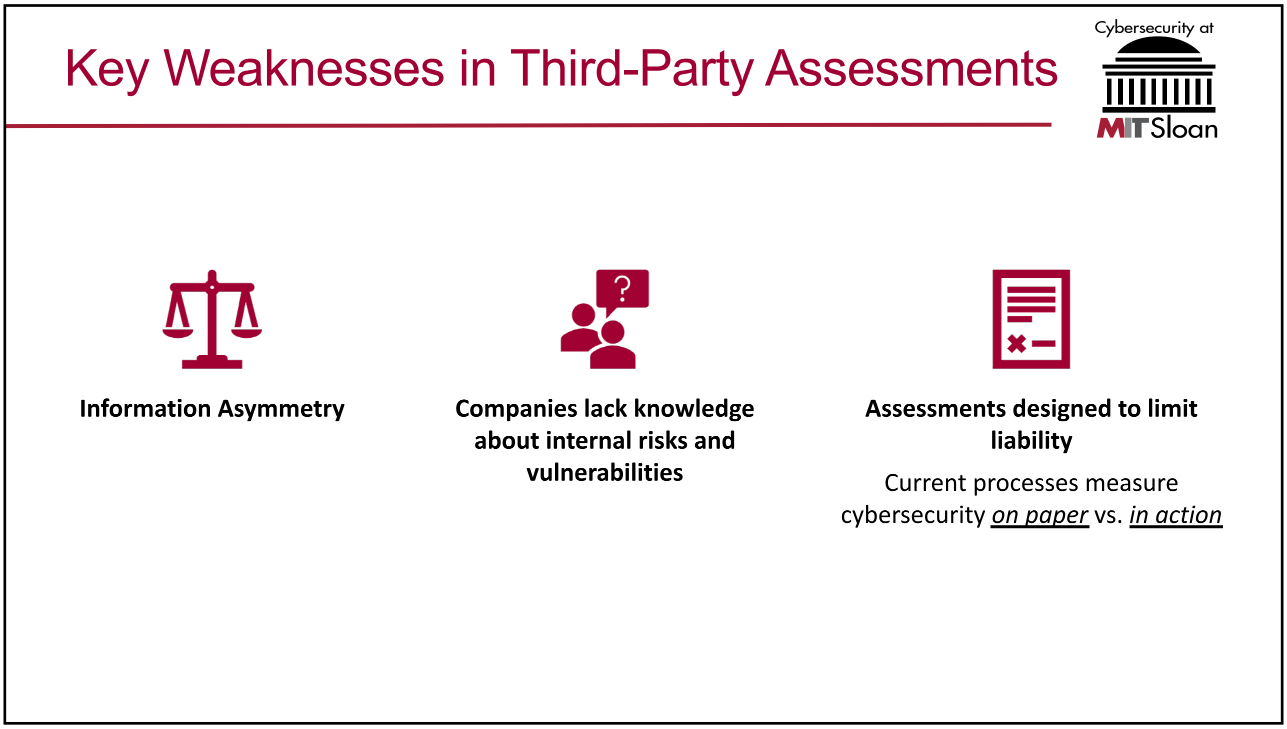


Questions

- ? What have you asked 3rd parties to do/how do you evaluate their security?
- What have you been asked to do as a supplier?
- What assessment tools/processes work well?
- Which of these assessment tools are most problematic for you? Why?

7

7



Key Weaknesses in Third-Party Assessments

Cybersecurity at
MIT Sloan

Information Asymmetry

Companies lack knowledge about internal risks and vulnerabilities

Assessments designed to limit liability

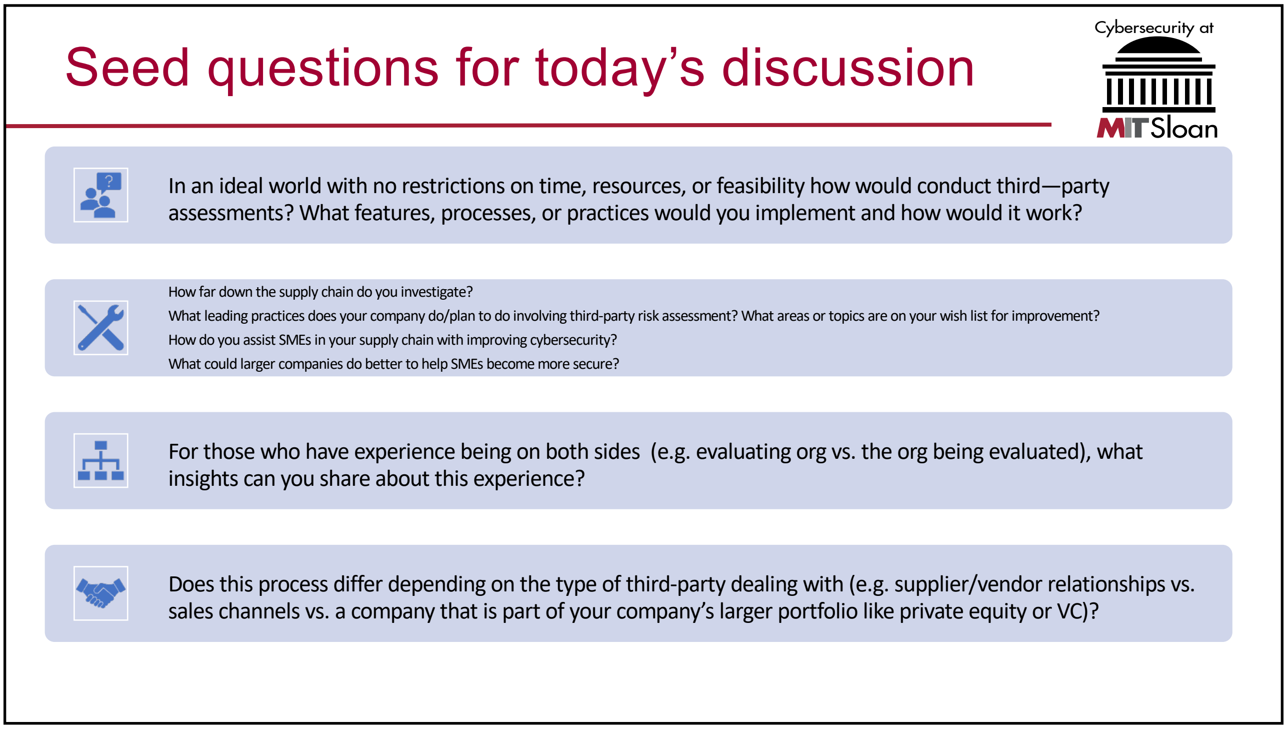
Current processes measure cybersecurity _on paper_ vs. _in action_

8

Discussion

9

9



Seed questions for today’s discussion

Cybersecurity at MIT Sloan

- In an ideal world with no restrictions on time, resources, or feasibility how would conduct third—party assessments? What features, processes, or practices would you implement and how would it work?
- How far down the supply chain do you investigate?
What leading practices does your company do/plan to do involving third-party risk assessment? What areas or topics are on your wish list for improvement?
How do you assist SMEs in your supply chain with improving cybersecurity?
What could larger companies do better to help SMEs become more secure?
- For those who have experience being on both sides (e.g. evaluating org vs. the org being evaluated), what insights can you share about this experience?
- Does this process differ depending on the type of third-party dealing with (e.g. supplier/vendor relationships vs. sales channels vs. a company that is part of your company’s larger portfolio like private equity or VC)?

10

Ways You Can Help

Cybersecurity at MIT Sloan

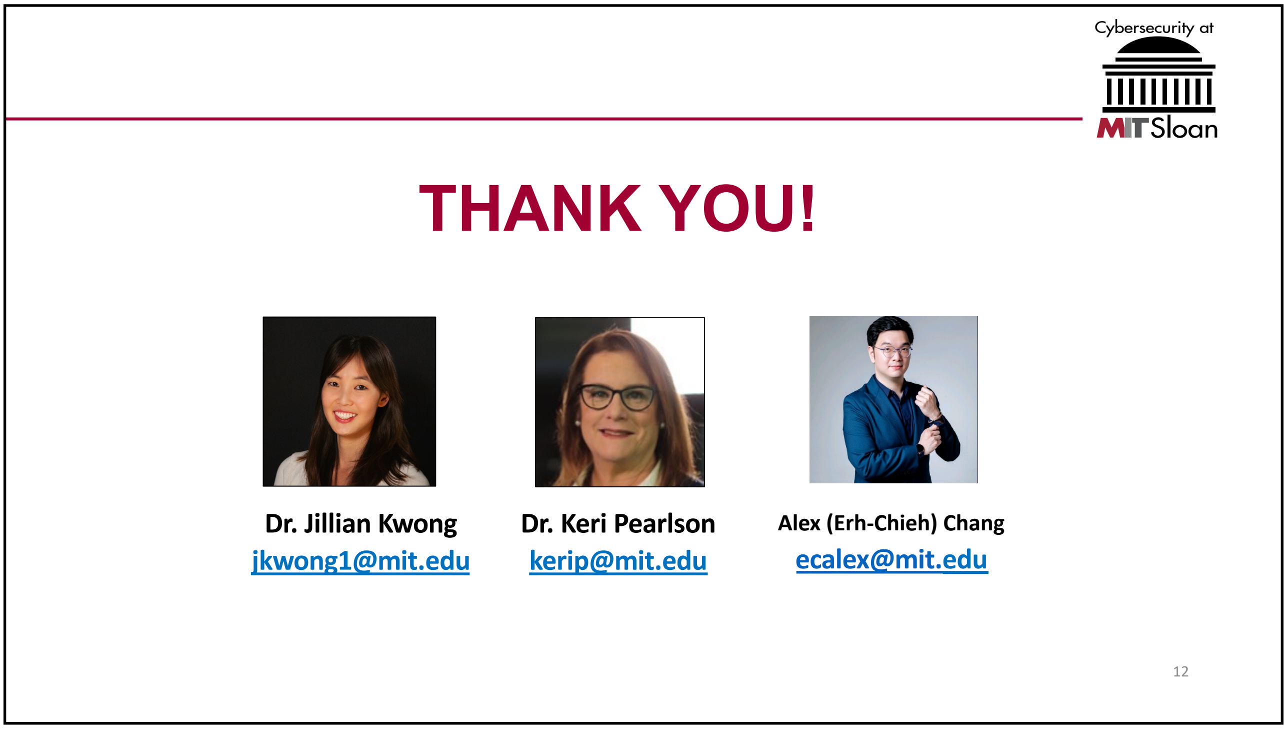
Research interview

Share your experience by participating in a short 30-60 minute research interview

Additional areas

Suggestions on people or resources that would be helpful to connect with

11



Cybersecurity at MIT Sloan

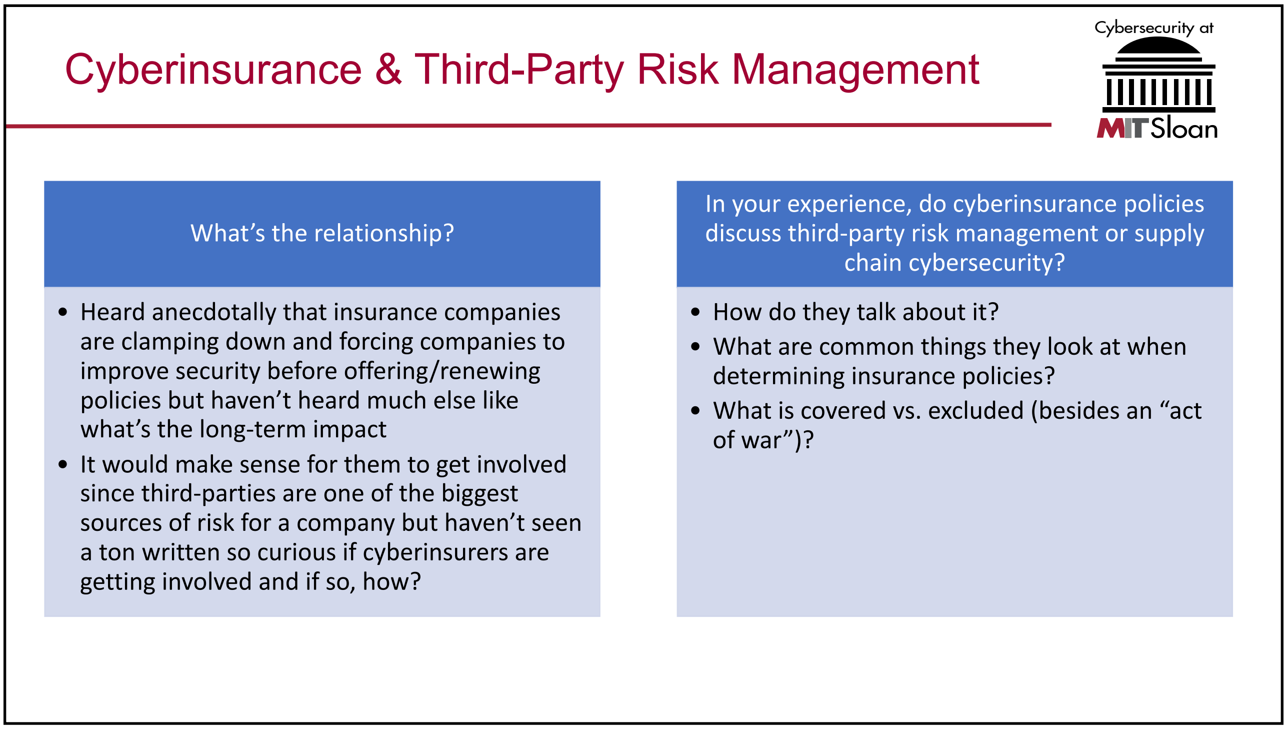
THANK YOU!

Dr. Jillian Kwong
jkwong1@mit.edu

Dr. Keri Pearlson
kerip@mit.edu

Alex (Erh-Chieh) Chang
ecalex@mit.edu

12



Cyberinsurance & Third-Party Risk Management

Cybersecurity at MIT Sloan

What's the relationship?

- Heard anecdotally that insurance companies are clamping down and forcing companies to improve security before offering/renewing policies but haven't heard much else like what's the long-term impact
- It would make sense for them to get involved since third-parties are one of the biggest sources of risk for a company but haven't seen a ton written so curious if cyberinsurers are getting involved and if so, how?

In your experience, do cyberinsurance policies discuss third-party risk management or supply chain cybersecurity?

- How do they talk about it?
- What are common things they look at when determining insurance policies?
- What is covered vs. excluded (besides an "act of war")?

13