1. Interconnectedness aggregates cyber risk

Security vulnerabilities in IT/OT networked business processes within critical infrastructures and enterprises increase their exposed risk to advanced persistent threats (APTs). This ultimately impacts business/society via aggregation effects along supply chains.

2. Innovating FAIR for IT/OT system (process) networks

We innovate the FAIR method in TWO aspects: (a) estimate enterprise cyber-loss profile from APT threat impacts, and (b) estimate cyber-loss profile for enterprise IT/OT infrastructure (process) networks (NWs). Our innovation helps to:

- Assess apriori, enterprise cyber-loss impact profile (via a Monte Carlo method).
- Organize and design business processes NWs that limit APT cyber-loss impact.
- Drive (a) enterprise table-top exercises to execute APT risk scenarios in IT/OT NWs and (b) cyber-protecting NW crown jewels to mitigate cyber-loss impact.

3. Finding: NW design influences loss impact

1. Enterprise susceptibility to security vulnerabilities within an adversary-aware IT/OT network influences first-party (FP) loss.
2. Star and Mesh IT/OT (process) networks reduce first-party loss.
4. Fat-tailed node degree statistics in SCNTs drive MP CAT risks.

4. Action items to boost resilience in IT/OT networks

(A) Network Architecture
Lower APT induced cyber-loss by:
2. Creating business process elements in clusters.

(B) Resilience via Insurance
1. Cyber-insurance boosts IT/OT resilience.
2. Light tailed loss distributions will be sustainable to coverage in the cyber-insurance market.
3. Heavy tailed loss distributions will not be sustainable to coverage in the cyber-insurance market.
4. Improve cyber-posture and culture to attract cyber-insurance providers.

(C) Network Security
Lower APT induced cyber-loss by:
2. Deploying anomaly detection solutions.
3. Effective network segmentation.
4. Block and/or filter unwanted network traffic.

(D) Resilience Planning
Plan ahead to lower APT cyber-loss by:
1. Network penetration tests.
2. Bug bounty programs.
3. Cyber-range exercises.

4. Action items to boost resilience in IT/OT networks

4. Action items to boost resilience in IT/OT networks

A tour of fat-tailed (Cyber-Loss, Node Degree) statistics

Plots are based on 100 K Monte-Carlo simulations using various loss distributions analyzed in our mathematical framework grounded in probability theory, random processes, network science, & statistics.

Contacts: ranjanp@mit.edu*, szeijl@mit.edu, msiegel@mit.edu

Illustration of fat-tailed cyber-loss impact. (α = fat tail degree) Illustration of fat-tailed node degree statistical distribution