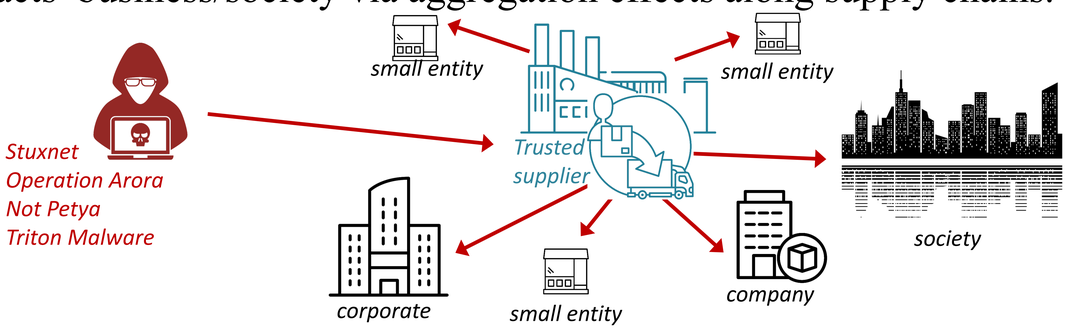
Boosting Resilience Within IT/OT Network Architecture

GOAL: To find the most resilient design choice of IT/OT network architecture subject to (aggregate) cyber-risk

Ranjan Pal, Sander Zeijlemaker, Michael Siegel

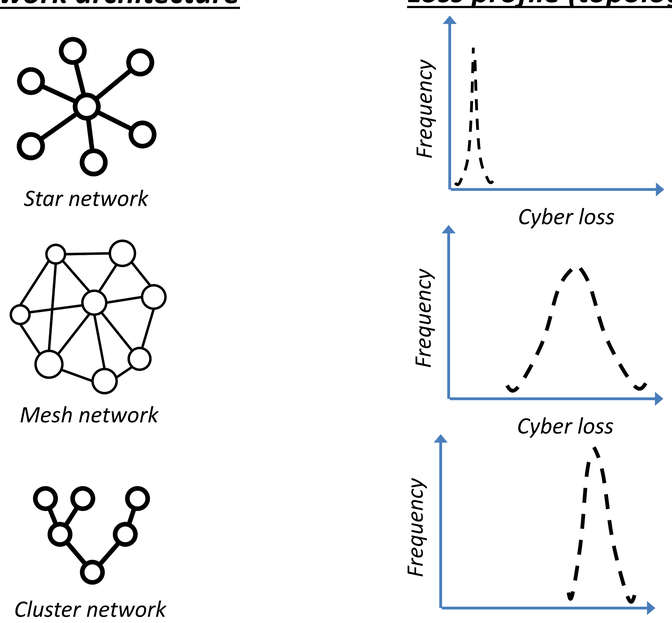
1. Interconnectedness aggregates cyber risk

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. IT/OT network design determines impact

Susceptibility of an enterprise to exploited vulnerabilities in adversary-known IT/OT networks determine the impact degree. In the worst case some architectures generate heavy tailed (multi-party) losses** upon the enterprise because key network architectural design strengths are leveraged by the adversary.



** Profiles are based on 100 K Monte-Carlo simulations using different loss distributions in our mathematical work grounded in statistical network theory, probability theory, network science and statistics.*

3. A methodical approach to estimates loss profile

Our 5-step approach enables to estimate your organizational (tail) loss profile from APT threats based on your IT/OT network design and helps to:

- Assess worst case loss impact scenario insights (with limited amount of data).
- Organize and design networked business processes that limit APT loss impact.
- Set priorities driving the security programs to help plan/re-imagine malware risk scenarios and mitigate this loss impact.

4. Learnings to boost resilience in IT/OT networks

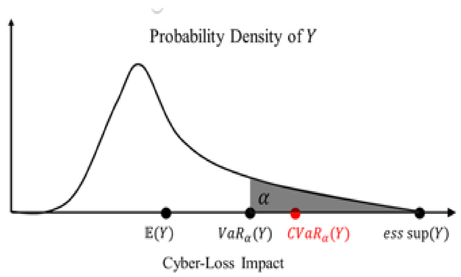
(A) Network Architecture

Lower APT induced cyber-loss by:

1. Creating star shaped networks.
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:

1. Strong vulnerability management & patching discipline.
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 bountry programs.
3. Cyber-range exercises.
4. Back-ups (data, code, state).

*** Figure aside shows a distribution of all possible degrees of cyber-loss impact. α = heavy tail.*

Looking forward to collaborate on boosting resilience in your organization's IT/OT network!

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