Decision Making in Ransomware Capability Development: Persona-Driven Simulation Approach

Prem Sagar, Sander Zeijlemaker, Michael Siegel

1. Ransomware threat grows

Loss from ransomware (Cybereason, 2022) :

- 67% of targets report $1 million and $10 million (USD), while
- 4% of them estimate impact on $25 million to $50 million.

Increasing threat:

- Factor 57 increase compared to 2015 (Freeze, 2021).
- Attributed 2021 damage: $20 billion dollars (Freeze, 2021).
- 60% to 80% private owned companies pay ransom (EP 2023).

2. Organizations struggle

CXO's are challenged by:

- The short-term dilemma of paying ransom; limit business disruption while funding the adversaries' business model.
- The long-term investment challenge to boost resilience and maintain financial performance.

3. Use simulation approach to mimic business environment

We leveraged the existing cybersecurity simulation management game (Jalali et al., 2019) and incorporated the following ransomware specific characteristics:

Business continuity

Integrates the domains of business continuity planning and disaster recovery initiatives to maintain performance.

Ransom payment dilemma

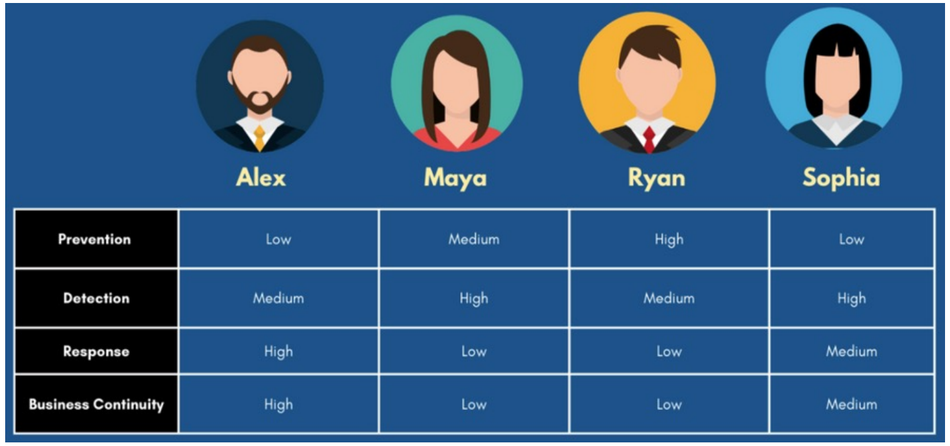
Embodies the intricate dynamics associated with ransomware payment decisions.

Controlling the spreading ransomware effects

Accounts for the lateral propagation of infection from compromised assets to vulnerable counterparts.

4. Mapping CXO's personas & resource allocation choices

Personas: artificial decision-makers profiles with specific characteristics that drive their cyber risk management strategy

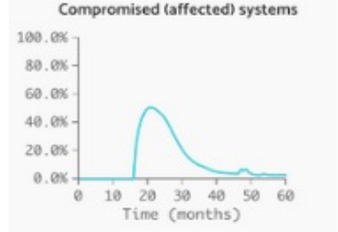


	Alex	Maya	Ryan	Sophia
Prevention	Low	Medium	High	Low
Detection	Medium	High	Medium	High
Response	High	Low	Low	Medium
Business Continuity	High	Low	Low	Medium

5. Paying ransom isn't the best strategy; business continuity is critical

Best profit scenario: Alex (not pay ransom)

Least spreading effect scenario: Alex (ransom not paid)



1%

Increase in resource allocation to business continuity efforts.

→

28%

Increase in profits (ransom not paid)

Paying ransom drives **short-term recovery** and *may* lead to **repeated attacks** which require continued recovery efforts

Looking forward to collaborate on boosting resilience against ransomware attacks?
Contact: szeijl@mit.edu, msiegel@mit.edu