Navigating the Cybersecurity Maze

Mikhail Falkovich

Director, Information Security

Consolidated Edison

Why Target Critical Infrastructure?

Threat Landscape

Who and Why?

- External sources
  - Terrorism
  - Hacktivism
  - Organized crime
- Internal sources
  - Disgruntled employees
  - Espionage

What and How?

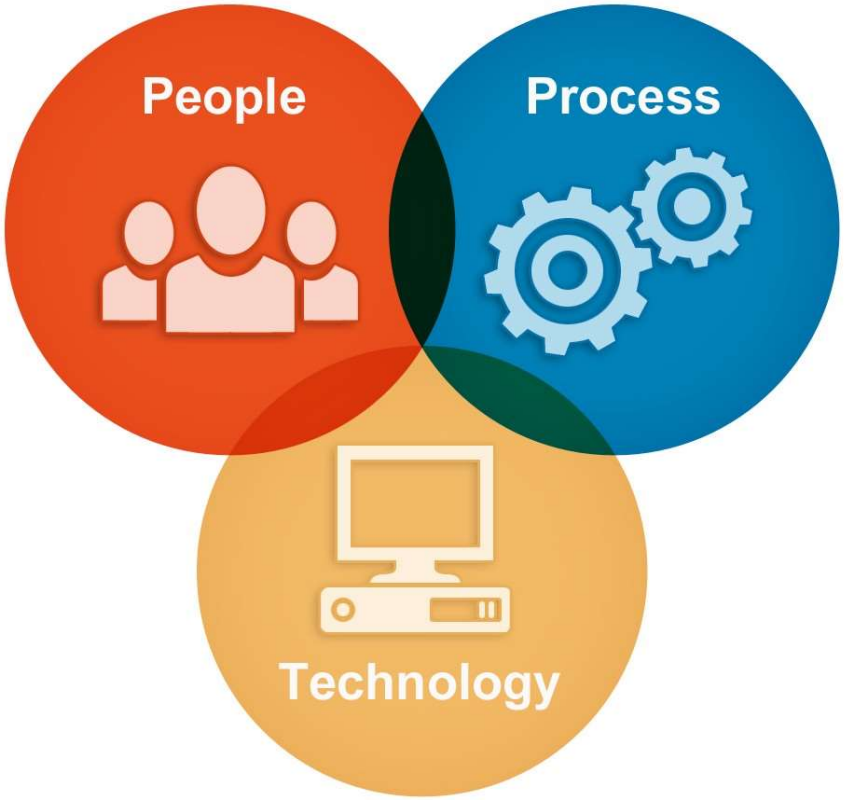
- Potential impacts
  - Data loss
  - Financial loss
  - Operational impact
  - Reputational impact
- Major Attack vectors
  - Social engineering/Phishing
  - Removable media
  - Vulnerability exploitation
  - Supply Chain / Partners

Core Cybersecurity Functions

CIA Triad

Cybersecurity Investments
Addressing Threats

- **People**
  - Awareness campaigns
  - Drills and tests
- **Process**
  - Threat intelligence/ information sharing
  - Response plans
- **Technology**
  - Defense in depth strategies
  - Security tools



Cybersecurity strategy
Mitigating the Risk

- Implement Defense-in-Depth and Defense-in-Breadth
  - Identify assets and minimize attack surface area
  - Implement layers of protections to protect systems/data
  - Utilize technology and process to identify anomalies
  - Respond to events
  - Practice incident response and recovery processes


Q&A