Tabletop Training and Coordination

RICK RIENSCHE
Asymmetric Resilient Cybersecurity Initiative Roadshow
May 12, 2017
Challenge

- Cyber defense presents a complex landscape
  - Initial ramp-up
    - New staff need to quickly understand how attacks work
  - Ongoing
    - Seasoned veterans must adapt to an ever-changing situation
    - Need to share knowledge within organizations and across organizations

- How do we keep up?
  - Lots of information available
  - Lots of “tribal knowledge”
  - *Above all else, we learn by doing*
Tabletop/role-playing exercise
- “If Dungeons & Dragons and Monopoly had a cyber baby…”

Players assume roles of the Blue Team
- Optionally, including differentiation between business and cyber roles

Players invest in technology and practices to defend their enterprise
- Investments represent a combination of dollars and time, abstracted to “resource tokens”

Simulated Red Team
- Subject matter expert “Game Master” acts as proxy
How the Game Works

► Gameplay
  ■ Investments drive changes to probabilities
    ○ Red team: probability of successfully completing a link in the attack chain
    ○ Blue team: probability of detecting Red’s activities
    ○ Probabilities and costs determined by extensive surveys
  ■ Players roll for success in various stages of the attack

► Record and debrief
  ■ Examine the decision-making process
Facilitates communication within and across organizations

Increasing awareness at all levels of decision-making

Can be tailored for a wide range of experience, expertise, and mission

- Engaging
- Collaborative
- Flexible
- Fun