Cybersecurity:
What Financial Officers Need to Know

01000100 01000001 01000110 01010000 00100000
01000011 01101111 01101110 01100110 01100101
01110010 01100101 01101110 01100011 01100101

What is cyberspace?

Cyberspace is the "[d]omain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures."

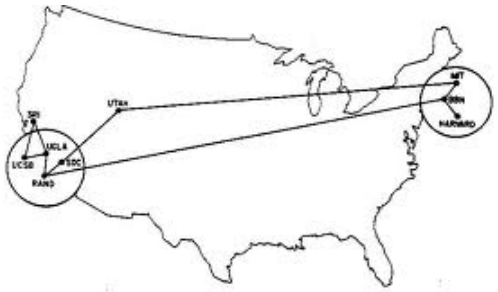
- National Military Strategy for Cyber Operations

Why are we concerned?

- Almost daily news about major breaches and loss of privacy
- Losses of intellectual property reach into the billions of dollars annually
- Growing security concerns over the threat to critical infrastructure

Why are solutions so hard?

- Not built with security in mind
  - Resiliency and efficiency were priorities
  - Lots of people eventually showed up with their valuables, with no one to protect them
  - Identity is difficult to ascertain

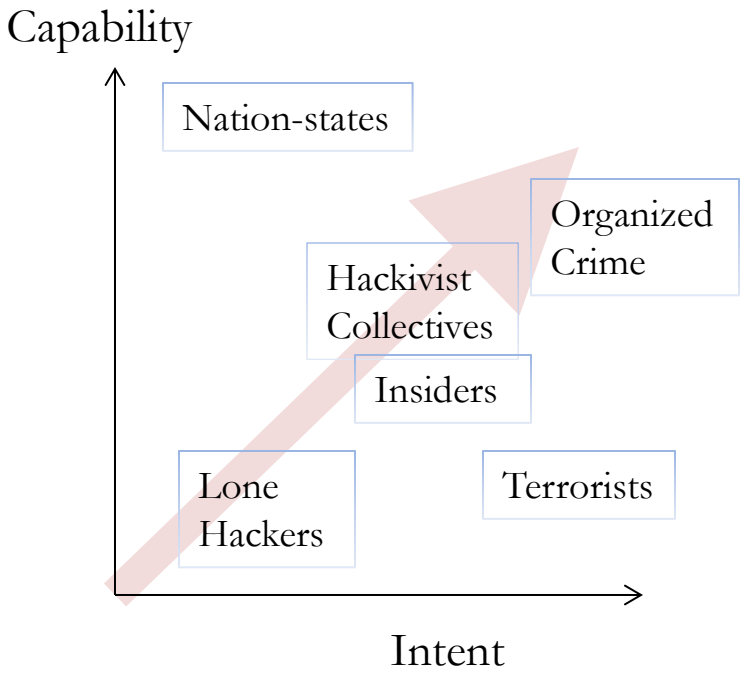


- As prey increase, so do predators (Lotka-Votterra Equation)
  - Prey are users, businesses, entertainers
  - Predators are advertisers, criminals, governments

- There are no nice neighborhoods on the Internet
  - Every criminal in the world is <500m/s away

Who's trying to harm us?

- Nation-states
- Sophisticated non-state actors
  - Eg: Organized Crime, Hacktivist Collectives
- Terrorists
- Lone wolf hackers
- Insiders



Current policy landscape

- Federal Legislation
  - Considering CIP, data breach, privacy, supply chain security, government reform, and information sharing
  - Private sector and public sector are distinct lines of effort but overlap
- Federal Regulation
  - First-party regulators are taking action in face of congressional inaction
  - SEC, FTC, FCC, and FERC/NERC are noteworthy
  - Agencies may use acquisition authorities to drive change
- State Actions
  - Mostly around privacy, CIP, economic development, education, and NG
  - Some states (like TX) have more robust activities, such as expert commissions

Technology trends

- Traditional solutions have focused on end-point-protection
  - Typically products focused on the user device
  - Eg: Symantec or McAfee/Intel
- Things have now progressed to network security
  - Firewalls, MSS, UTM
  - Eg: FireEye, PAN, CSPs
- CISOs are now looking beyond network security
  - Necessary but insufficient. Instead, assume breach and protect data
  - Heuristic analysis, virtualization, data security, etc
  - Firms also grappling with cloud employment and more nuanced strategies

Recommendations

- Think about information security in broader terms
  - Not just a tech issue but also impacts enterprise risk and competition
- Develop an overall strategy
  - Find the right technology solutions but also think about how your systems are architected, user accesses, and what's most valuable
  - Think carefully about how to balance privacy, security, cost, and efficiency
- Keep up with market and policy trends
  - Malware and defenses are both evolving rapidly
  - The policy landscape may change quickly in response to an event
  - Insurance and legal liability doctrine are also maturing
    - Finance, defense, and health case industries will be particularly impacted

Tips on talking with your board

- Boards, in their governance capacity, have a business perspective
  - Getting board support requires providing the whole business story (eg: cost, mitigation, impacts)
  - Make it easy to understand (score cards and dashboards)
  - Talk about risks, threats, and potential solutions

- Extrapolate points quickly, distill, and present
  - This is a challenge with the volume of information today
  - Presenting is as much about managing time as information

- After an incident, discuss the issues frankly
  - Avoid discussion of blame and present the facts
  - Focus on impacts and remediation

Questions?