FEDERAL RESERVE BANK OF BOSTON™

Securing the Financial Services Supply Chain

January 20, 2016

Don Anderson
Senior Vice President &
Chief Information Officer
Federal Reserve Bank of Boston

Why does this matter?

- Stolen Checks
- Money Laundering
- Impersonation
- Fraudulent loans
- Robbery

$400B

$???

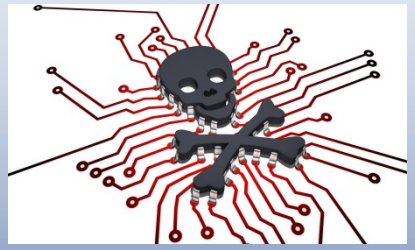
- Identity Theft and Personal Data
- Payments Fraud
- Espionage
- Unauthorized Access
- Intellectual Property

Escalating Threat

Criminal Activity

Financially motivated criminal activity continued to increase through 2013 and 2015 with frequent activity in the Critical Infrastructure (Utility, Water, Communication, etc..) and Information Industries. A wider range of hacker toolkits have become available and sustained improvements in criminal capability is compounding existing issues.

Rogue Nation States



In the face of improving criminal capability, organizational incident response times and effectiveness at detecting network intrusions have remained relatively static. Rogue states tend to be driven by political and ideological motivations, aiming to cause disruption and financial loss to a given target, rather than achieve personal gain.

Prioritization and “The Shift”

A successful cyber attack could be…

→ Strategic	→ Operational	→ Reputational
• Prevent the organization from achieving its mission • Displace the organization in the industry	• Unable to conduct business processes • Manipulate a business process to the attacker’s advantage	• Lose faith in the brand

Impact of Cyber Crime

But what is the real impact?

- Are human and financial resources being used most effectively?
- Are portions of the population unlikely to leverage technology?
- What is the impact on financial stability?

Impact of Innovation on Payments

+ Lower costs and more flexible payments options for consumers and businesses

- Cyber-security issues are beginning to ***intrude on the benefits*** of some of these innovations

Small banks – risk, but little reward

Innovation is coming from new vendors, in unregulated industry at a high velocity

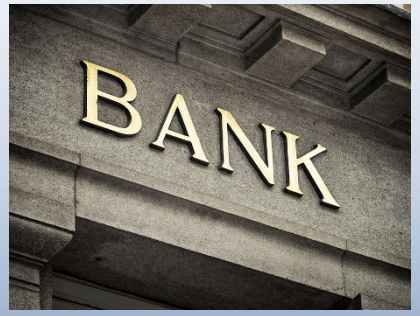
Competing Forces

Cyber disruption or loss

Digital disruption / New Products, services and competitors

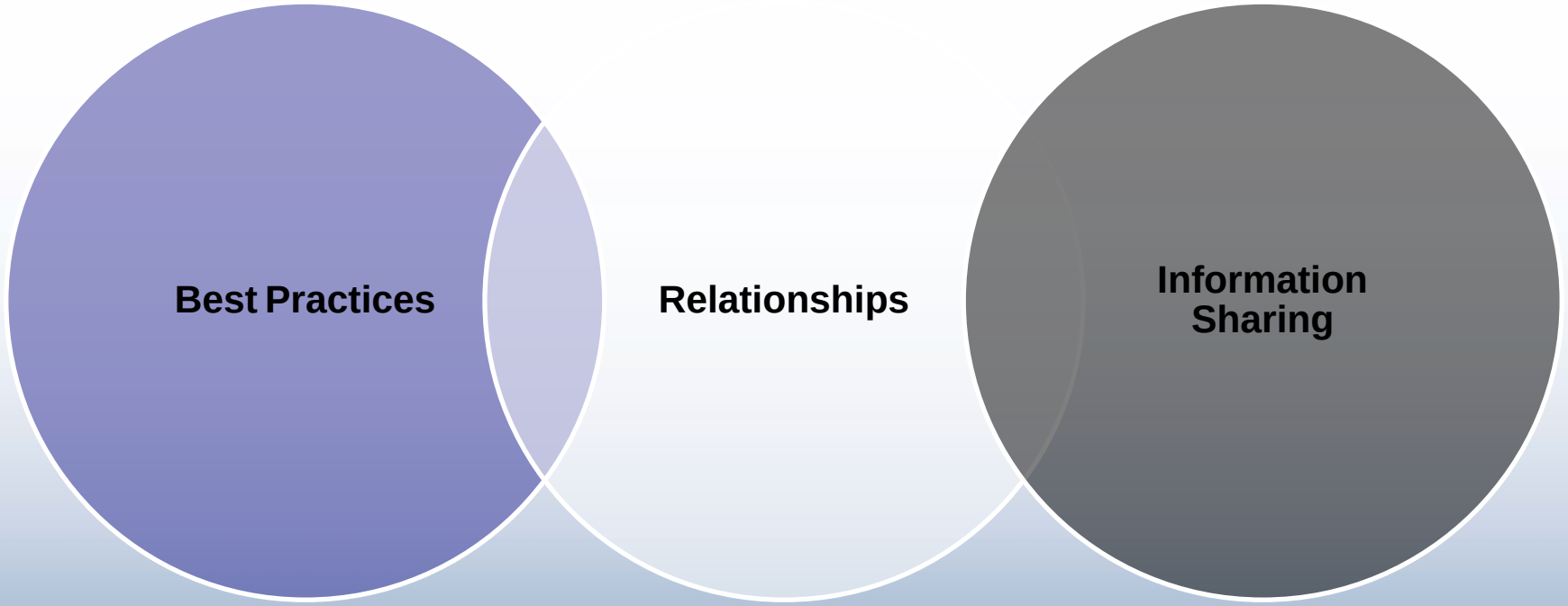
Compliance with regulations

Service to customers and owners



Can We Solve It?

NO



Best Practices

- ✓ Overlap of controls (Defense in Depth, employee awareness, patching, employee training, etc..)
- ✓ Table top various scenarios
  - Can we live without the Internet? Or computers?
- ✓ Look inside, not just outside (malicious or accidental)
- ✓ Adopt standard security program as a baseline (NIST, ISO, ENISA, etc.)
- ✓ Continue to invest in new technology, people and skills

Relationships

- Establish relationships now and get agreements in place to have candid conversations.
- Key relationships
  - Vendors / Partners / Supply Chain
  - Law Enforcement
  - Auditors / Regulators
  - Competitors
  - Academic / Research and Development (R&D)

Information Sharing

Example at the Federal Reserve Bank of Boston

- Single-industry focused program
  - Information sharing is the key component
  - In-person meetings – everyone signs non-disclosure (NDA) forms and commits to keeping discussion confidential
  - Conducted by cyber-security experts within the Federal Reserve who have broader access to details about emerging threats and mitigations than may be available to smaller financial institutions
  - Not part of the supervisory / regulation process

Next Frontier

- Cyber Resiliency
  - Identify dependencies and criticality
  - Prioritize recovery
- Cloud Risk Management
  - Ensure 3rd party is at least as secure as you
  - Don't lose the benefits of speed and agility

Conclusion

1. The rate in terms of frequency and impact of cyber crime will continue to grow and accelerate
2. Innovation and regulation are not synchronized
3. Everyone in supply chain needs to address and manage risk continuously
4. All need a plan to react and respond **WHEN** an attack occurs

DISCUSSION