Emerging Leaders in New England’s Banking Industry

June 2, 2017

Kenneth Montgomery
First Vice President & COO
Federal Reserve Bank of Boston
Mission

The Federal Reserve System is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system. Over the years, its role in banking and the economy has expanded.

Today, the Federal Reserve’s duties fall into four general areas:

• Conducting the nation’s monetary policy by influencing the monetary and credit conditions in the economy in pursuit of maximum employment, stable prices, and moderate long-term interest rates

• Supervising and regulating banking institutions to ensure the safety and soundness of the nation’s banking and financial system and to protect the credit rights of consumers

• Providing financial services to depository institutions, the U.S. government, and foreign official institutions, including playing a major role in operating the nation’s payments system

• Maintaining the stability of the financial system and containing systemic risk that may arise in financial markets
The Federal Reserve’s Federated Structure

12 Districts

1. Boston
2. New York
3. Philadelphia
4. Cleveland
5. Richmond
6. Atlanta
7. Chicago
8. St. Louis
9. Minneapolis
10. Kansas City
11. Dallas
12. San Francisco

Board of Governors

Washington, D.C.

Geographic Boundaries of the Federal Reserve Districts
High Profile, High Intensity Cyber Attacks
Increasing Impact on Central Banks and Financial Services

- U.S. Bank Regulator Notifies Congress of Major Data Security Breach
  Office of Comptroller of Currency discloses unauthorized removal of more than 10,000 records.

- Reserve Bank of India (RBI) to Ethically Hack Into Banks to Find Vulnerabilities

- Swift Releases New Controls, Suspicious-Payments Blocker
  Moves come as committee of central banks prepares international guidelines on payment-security responsibilities.

- Suspects arrested in Russia central bank cyberheist: bank official
  Exclusive: Bangladesh police detail suspicions of inside help in central bank heist

- Italy arrests two for hacking into emails of ECB's Draghi, former Italy PM Renzi

- U.S. may accuse N. Korea in Bangladesh cyber heist: WSJ

- BlackEnergy Hackers Now Launching Attacks Against Ukrainian Banks

- Exclusive: SWIFT confirms new cyber thefts, hacking tactics

- Google Team Cracks Longtime Pillar of Internet Security
  Researchers at Alphabet unit, Dutch institute demonstrated ‘collision attack’ on cryptographic technology known as SHA-1

- Cobalt Gang Makes ATMs Across Europe Spew Cash

- Invisible Malware Found in Banking Systems in over 40 Countries

- WannaCry Ransomware That's Hitting World
  Right Now Uses NSA Windows Exploit

- 20,000 Tesco Bank accounts raided by hackers, money stolen

- U.S. accuses Chinese citizens of hacking law firms, insider trading

- Alleged NSA hack group Shadow Brokers releases new trove of exploits

- Ongoing DDoS Attack Against DynDNS
  Knocks Major Services Offline

- Lloyds bank accounts targeted in huge cybercrime attack

- Thieves drain 2fa-protected bank accounts by abusing SS7 routing protocol

- WikiLeaks says it has obtained trove of CIA hacking tools
High Profile – High Intensity Illustrative Cases

SWIFT Network
- February 2016 – Instructions to transfer $951 million from Bangladesh Central Bank from an account at the Federal Reserve Bank of New York via the SWIFT network. $101 million was transferred before being stopped.
- Confirmed reports of Banco del Austro (Ecuador), commercial banks in Ukraine, Vietnam and potentially dozens more.

Distributed Denial of Service Attacks (DDoS)
- Large number of computers, under the control of an adversary, overwhelm a computer, website or application.
  - 2013 - large scale attacks impact the operations of a number of large banks.
  - 2014 to 2016 - DDoS mitigation services become mainstream minimizing the impact.
- September 2016 - Mirai Malware – 1,000 times more powerful.

Ransomware
- Impact: 40% of businesses impacted by ransomware (30% lost revenue as a result, 20% had to cease business operations)
- Cost (60% of ransomware attacks demanded over $1,000; 20% over $10,000; 1% over $150,000)
- Protection (96% of organizations are not confident they can stop malware; 79% of organizations are not confident in their backups)
- WannaCry: Over 200,000 Infections in 150 countries; Revenue only ~$85k
- Profitable Ransomware Examples: Locky - $220M; Cryptowall - $100M; CryptXXX - $73M
Use of Technology Increasing

- Replacement of core banking functions with technology
- Mobile Banking / Payments
- Financial Technology (FinTech)
- Blockchain / Distributed Ledger Technology (DLT)
  - Hub and spoke – peer to peer
  - New trust models
  - More interconnected networks
Boston Fed Cyber Threat Sharing Series

1. Trusted Forum of Peers
   - Similar Challenges
   - Share Problems and Solutions

2. Threat Sharing
   - Consolidated
   - Targeted
   - Actionable

3. Guest Speakers
   - Emerging Trends
   - Areas of Focus

4. Best Practices
   - Subject Matter Experts
   - Topics of Interest

5. Member Roundtable
   - Sounding Board
   - Current Issues
   - Creative Solutions

Yearly Highlights:

- **2014**: Pilot Begins, 20 Participating Organizations
- **2015**: 40 Participating Organizations, Discussion Forum Added to Portal
- **2016**: 60 Participating Organizations, First Cybersecurity Conference
- **2017**: Continued Growth in Membership, Pilot of Satellite Model, FinTech Expansion
Conclusion

Cyber Risk is Real, Disruptive, and Increasing in Impact/Complexity

Central Banks and Financial System are Key Targets: Interconnectedness Now a Financial Stability Risk

Business Models Will Evolve in Response to New Technical Demands and Cyber Risk

Cyber Risk is an Enterprise Risk Warranting Director Level Reporting, Oversight, and Expertise