FEDERAL RESERVE BANK OF BOSTON™

Cyber Threat Sharing

November 10, 2015

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

Background

Driving Factors

Implementation of a cohesive information security strategy continues to become both more costly and complex.

Increasing numbers of organizations are confronting strategic decisions on how best to secure their companies' most important assets.

Call to Action

At a 2013 meeting of the Federal Advisory Committee to the Federal Reserve Board of Governors, members discussed the inability of US depository institutions (DIs) to effectively share cyber-threat information between one another.

Members noted: the Fed could expand its role by providing cyber security advisory services as a trusted interlocutor between banks and other government agencies.

Federal Reserve Capability

The Federal Reserve Bank of Boston has both local and national expertise in cyber security and threat sharing experience as a member of the Advanced Cyber Security Center (ACSC).

In addition to playing a role as a convener, there will be a role for the Fed in helping organizations with cyber security as well.

The Solution

- Multilateral non-disclosure agreement amongst participants
- Separate from Supervision and Regulation
- Threat Sharing Group
  - Bi-weekly meetings (in person and virtual)
  - Sharing portal
  - Focus: Information Sharing, Best Practices, Special Topics
- Quarterly Seminars
  - Emerging threats and research
- Annual Conference
  - Trends and Industry Perspective

Key Benefits

* Size of circle indicates number of times specific benefit was mentioned by banking industry participants, during focus groups.

For More Information

Jasvinder Khera – Security Systems Engineer

Jasvinder.Khera@bos.frb.org

(617) 973-2934

Don Anderson – SVP & CIO

Don.l.Anderson@bos.frb.org

617 973-3926