Evolving IT Risks
Quarterly Conversations with the Fed Call
November 13, 2013

Presented by Joe Brennan and John Bargiel
Federal Reserve Bank of St. Louis
Disclaimer

The information contained in this presentation is the opinion of the presenters and does not necessarily reflect the views of the Federal Reserve Bank of St. Louis or of the Federal Reserve System.
Agenda

• Top information technology (IT)/Operations risk for banks
  – What is the risk?
  – Why should banks care?
  – What is the threat profile?
  – What can merchants do?
  – What can banks do?
• Additional resources
Top IT/Operations Risk for Banks
Merchant Account Take Over

The merchant
• Wide spectrum of information security aptitude
• In most cases no regularity oversight
• Weak or non-existent internal audit function

The financial institution (FI)
• Fundamentally sound information security practices
• Regulatory oversight
• Audit function
Why Should Banks Care?

Risk: Reputational, financial, legal, operational, regulatory

Village view escrow (March 2010)
• Merchant lost $466,000 and compensated $600,000.

PATCO Construction (May 2009)
• Merchant compensated for original loss plus interest.

The moral of the story is that the financial institution was stuck with the bill.
What Is the Threat Profile?

Looking to score easy points
- Low level of technical skills
- Focused on weakest link, not hard targets
  - 33 percent of organizations have less than 250 employees.

Only in it for the money
- Organized crime, not state sponsored
- Not interested in espionage or cyber terrorism
- Will typically run if disrupted and not “go to ground”
What Can Merchants Do?

Protect, Detect, Respond

Ideally at dedicated Internet banking terminal
- No web surfing
- No email
- No administrative rights
- No wireless connection
- No external media connection
- All security patches up to date
- Antivirus and malware protection
- Firewall

Social engineering

All known authentication measures can be defeated if the end points are not secure.
What Can Merchants Do? (cont.)

Protect, Detect, Respond

Detect:
• Daily account reconciliation
• Warning signs: Slow workstation and rogue emails

Respond:
• Documented incident response plan
What Can Banks Do? (cont.)

Protect, Detect, Respond

- Consider the same endpoint protections on personal computers (PCs) as merchants
- Update the risk assessment annually or when there are changes in payment channels
- Develop baseline security controls for merchants
- Implement ongoing security awareness education for retail and high risk business transactions
- Establish bank controls to mitigate risk of CATO (corporate account takeover)
- Contact your vendors to regularly receive information regarding reducing the risk of CATO
What Can Banks Do? (cont.)

Protect, **Detect, Respond**

- Establish automated or manual monitoring systems
- Educate bank employees of warning signs that a theft may be in progress
- Educate account holders of warning signs of potentially compromised computer systems
- Update incident response plans to include CATO
- Implement a contingency plan to recover or suspend any systems suspected of being compromised
- Contact law enforcement and regulatory agencies once the initial recovery efforts have concluded
- Implement procedures for customer relations and documentation of recovery efforts
What Can Banks Do? (cont.)

The FI: Common exam findings

Vendor management
• Risk cannot be outsourced

Access reviews
• Least User Access (LUA)

Vulnerability scanning
• Valuable tool in discovering vulnerabilities in network, PCs, servers, and hardware

Patch management
• SR 13-16 End of Microsoft support for Windows XP
Questions

*1 on your phone
or
rapid@stls.frb.org
Additional Resources

Texas Bankers Electronic Crimes Task Force
• http://www.ectf.dob.texas.gov/ectftools.htm

Supervisory Letters
• http://www.federalreserve.gov/bankinforeg/srletters/srletters.htm

Microsoft resources-End of support

Case study: PATCO Construction
• http://www.bankinfosecurity.com/patco-settlement-what-means-a-5373/op-1

Case study: Village View Escrow
• http://www.pcworld.com/article/258310/california_business_scores_settlement_in_thorny_cybercrime_case.html

Case study: Dissecting Operation Troy

Case study: Dissecting Operation High Roller