Cybersecurity
A Regulatory Perspective

Sara Nielsen
IT Manager
Federal Reserve Bank of Kansas City

The opinions expressed are those of the presenters and are not those of the Federal Reserve Banks, the Federal Reserve System, or its Board of Governors.

Topics

- IT Trends
- Regulatory Guidance
- InTREx
- Common IT Exam Findings
- Payments Fraud

Information Technology Trends

Information Technology Trends

- **Existing vulnerabilities continue to be exploited**
  Easily exploitable vulnerabilities persist

- **New platforms create new cyber attack opportunities**
  New ways to exploit financial institutions and their customers

- **Lines between cyber actors are blurring**
  Commercialization of tools, resources, and infrastructure

Information Technology Trends (cont'd)

- **Tactics evolve in response to online behavior**
  Social networks enable more effective and targeted attacks

- **Trends in malware are evolving**
  Destructive malware and cryptographic ransomware

- **Global unrest results in changing motivations**
  Regions that either have cyber capabilities or resources to purchase them may turn their focus towards the U.S. financial institutions during political and social unrest

Information Technology Trends (cont'd)

Potential Impacts

- Financial
- Operational
- Legal
- Reputational

Cybersecurity
FFIEC Regulatory Guidance
Recent Notifications

Regulatory Guidance Cybersecurity of Interbank Messaging and Wholesale Payment Networks

BACKGROUND

- Recent cyber attacks against interbank networks and wholesale payment systems to commit fraud have demonstrated capability to:
- Compromise a financial institution's wholesale payment origination environment, bypassing information security controls
- Obtain and use valid operator credentials with the authority to create, approve, and submit messages
- Employ sophisticated understanding of funds transfer operations and operational controls
- Use highly customized malware to disable security logging and reporting, as well as other operational controls to conceal and delay detection of fraudulent transactions
- Transfer stolen funds across multiple jurisdictions quickly to avoid recovery

RISKS

- Unauthorized transactions involving interbank messaging and wholesale payment networks may subject the originating bank to financial loss and compliance risk

Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network

Society for Worldwide Interbank Financial Telecommunication

Regulatory Guidance Cyber Attacks Involving Extortion/Ransomware

BACKGROUND

- Cyber criminals and activists use a variety of tactics, such as ransomware, denial of service (DoS), and theft of sensitive business and customer information to extort payment or other concessions from victims
- In some cases, these attacks have caused significant impacts on businesses' access to data and ability to provide services
- Other businesses have incurred serious damage through the release of sensitive information

RISKS

- Financial institutions face a variety of risks from cyber attacks involving extortion, including liquidity, capital, operational, compliance and reputation risks, resulting from fraud, data loss, and disruption of customer service

Regulatory Guidance Ransomware

Regulatory Guidance Destructive Malware

BACKGROUND

- Over the past two years, cyber attacks on businesses have increased in frequency and severity
- In some cases, destructive malware used in these attacks successfully compromised large quantities of data and rendered supporting systems inoperable
- Malware can be introduced into systems through a variety of mechanisms, including through employees downloading attachments in phishing or spear-phishing emails, connecting external devices (e.g., USB drives), or visiting compromised Web sites, or through unauthorized parties using stolen employee or third-party credentials to install malware directly on systems
- Once introduced, destructive malware may be further distributed through compromised enterprise system management technologies

RISKS

- Financial institutions face a variety of risks from cyber attacks involving destructive malware, including liquidity, capital, operational, and reputation risks, due to such events as fraud, data loss, and disruption of customer service

Data Breaches

Regulatory Guidance
Risk Mitigation Practices

- Securely configure systems and services
- Review, update, and test incident response and business continuity plans
- Conduct ongoing information security risk assessments
- Perform security monitoring, prevention, and risk mitigation
- Protect against unauthorized access
- Implement and test controls around critical systems regularly
- Enhance information security awareness and training programs
- Participate in industry information-sharing forums

Cybersecurity
FFIEC Regulatory Guidance (CAT)

FRB SR Letter 15-9
FFIEC Cybersecurity Assessment Tool

Overview for Chief Executive Officers and Boards of Directors

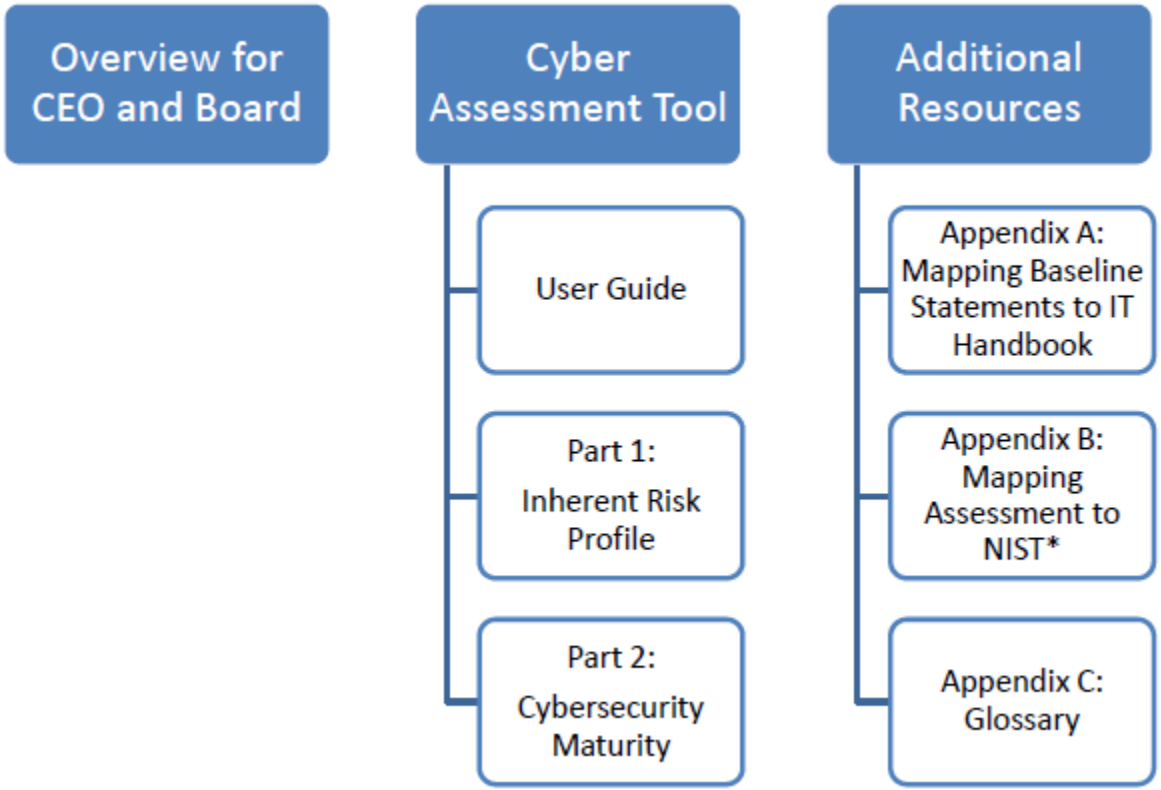
In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council(FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. *The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.* The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

CAT Parts and Process

The Assessment consists of 3 major components:

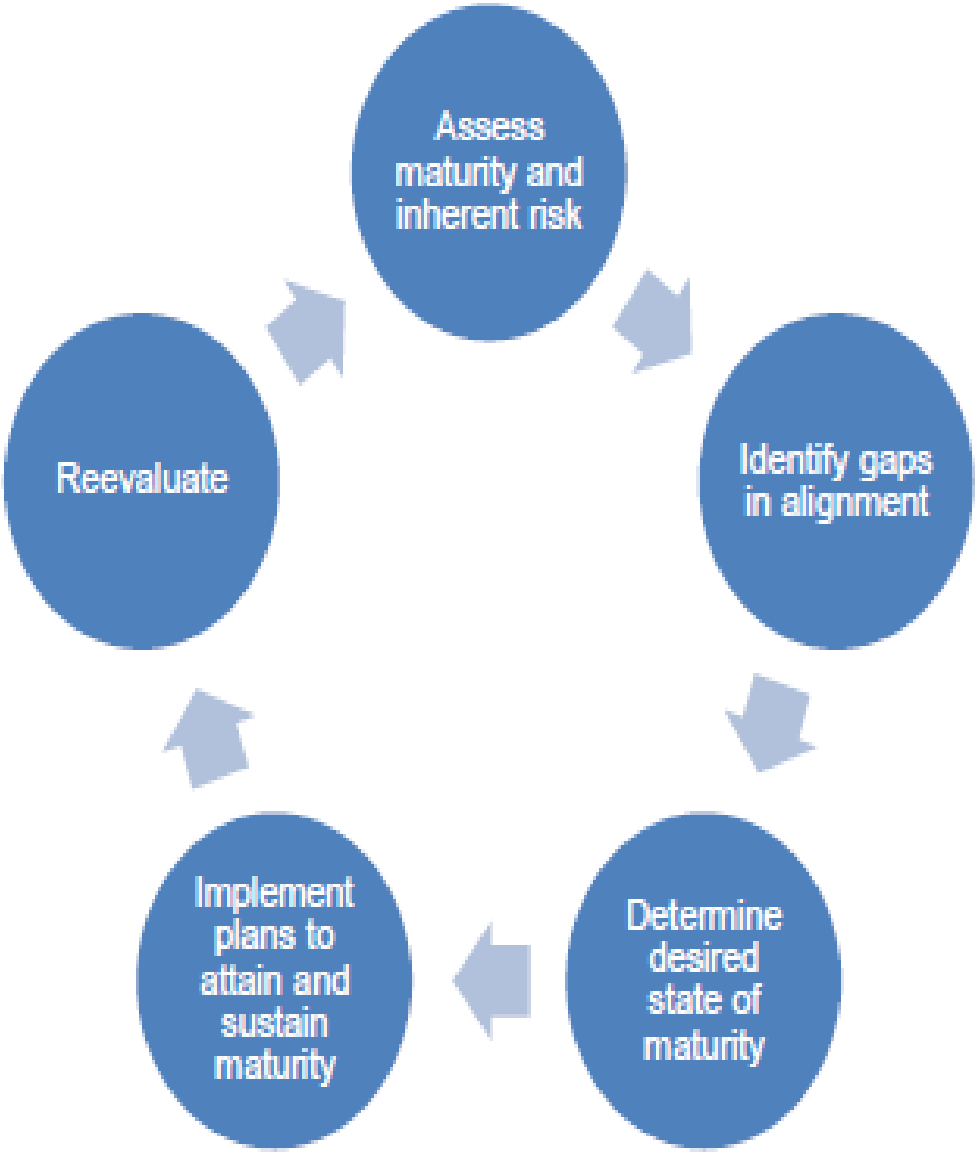
1. Inherent Risk Profile- rating your inherent risk for cybersecurity threats based on your size and complexity
2. Cybersecurity Maturity- regarding how prepared you are to handle different cybersecurity threats
3. Interpreting and analyzing your results by understanding how your inherent risk ties to your cybersecurity maturity, and where you should be regarding risk vs. maturity

Assessment Tool Components

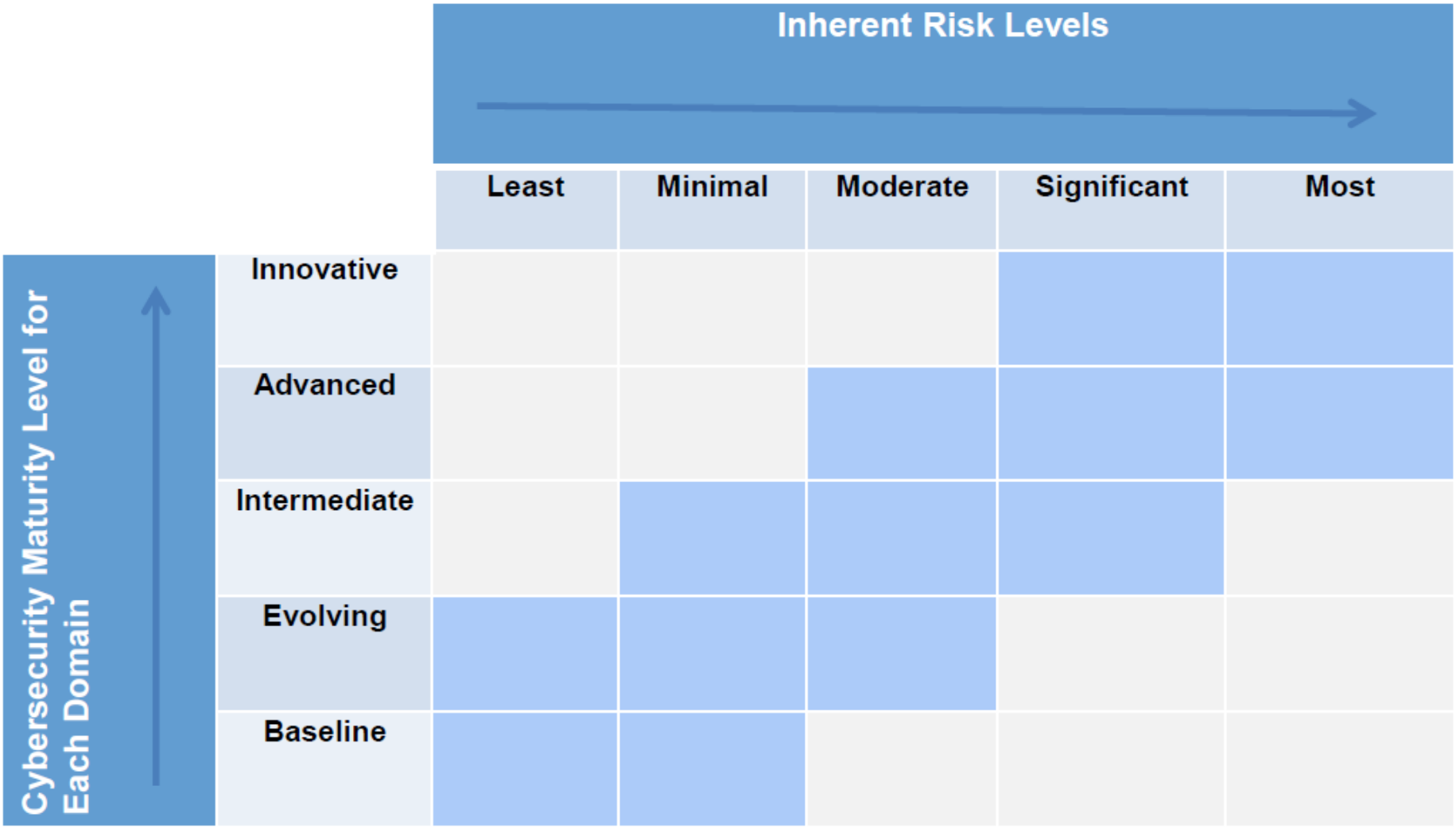


CAT Tool Steps

1. Complete Part One: Inherent Risk Profile
2. Complete Part Two: Cybersecurity Maturity Assessment
3. Determine appropriate target maturity level
4. Identify any gaps between current and desired states
5. Develop implementation plans based on identified gaps



Cybersecurity Assessment Tool Risk Matrix



InTREx
Information Technology
Risk Examination Program

InTREx

- The FRB, FDIC and CSBS updated information technology and operations risk (IT) examination procedures to provide a more efficient, risk-focused approach
- This enhanced program also provides a cybersecurity preparedness assessment and discloses more detailed examination results
- The InTREx Program is an enhanced, risk-based approach for conducting IT examinations
- The Program helps to ensure that financial institution management promptly identifies and effectively addresses IT and cybersecurity risks

InTREx Program

IT Profile

Work Programs

Audit Management

Development & Acquisition Support & Delivery

InTREx (cont'd)

- The Core Modules incorporate procedures to assess compliance with Appendix B to Part 364 of the FDIC Rules and Regulations entitled *Interagency Guidelines Establishing Information Security Standards* as well as procedures to assess cybersecurity preparedness

- The results of these assessments will be embedded in the Report of Examination

InTREx (cont'd)

- The complete InTREx program is available through the FDIC's website:

- Financial Institution Letter
  - FIL-43-2016
  - June 30, 2016

Cybersecurity Exam Expectations

- All firms must complete a comprehensive cybersecurity risk assessment
  - Use of the CAT is not required
- All firms must comply with the baseline expectations of the FFIEC IT Handbooks
  - Outlined within Appendix A of the CAT

Cybersecurity Governance Expectations

Expectation	Governance
Risk Assessment	Review at least annually Approve and support plans to address gaps
Compliance with Baseline Expectations	Review at least annually Support management in maintaining full compliance with baseline expectations and achieving higher levels of risk management, as needed
Incident Response Planning	Review as needed Ensure plans are comprehensive, realistic, and tested
Training of Staff	Review reporting of training at least annually Support comprehensive training, including social engineering prevention strategies
Testing/Patch Management	Review results of tests and audits as conducted Ensure issues are fully addressed in a timely manner Ensure patches are current
Information Sharing	Review as needed Stay aware of trends and risks in cybersecurity

Common IT Examination Findings

Common IT Exam Findings

- Control Weaknesses
  - Overly broad access levels
  - Excessively high wire transfer approval limits
  - User access rights are not roles based
  - Too many network administrators
  - Failure to terminate user rights upon separation

- Data/Asset Management
  - Exclusion of some assets in risk assessments
  - Not diagraming networks
  - Failure to patch software in a timely manner
  - Lack of internal network scans

Common IT Exam Findings (cont'd)

- IT Governance
  - Failure to comprehensively report to board
  - Wire/ACH limits are not reviewed/approved by board
- Information Security
  - Need for comprehensive GLBA reporting
  - Failure to properly control/manage PII leaving the bank
  - Need to complete social engineering testing/training

Payments Fraud and Lessons Learned

Payments Fraud

- Payments fraud is on the rise
  - Law enforcement agencies are all reporting a significant increase in funds transfer fraud
  - Online banking credentials of small/medium sized businesses are being exploited
- Wire fraud incidents are prevalent across the region
- Account take over example
- Bank system malware example

Payments Fraud (Cont'd)

- **Fraud lessons learned**
  - Ensure your organization has:
    - Strong controls
    - Effective policies/procedures
    - Appropriate risk limits
    - Policies consistently followed
    - Strong exception approval process
    - Social engineering training
    - Social engineering testing
    - Testing/auditing of staff's adherence to policies

Resources

Threat Intelligence Information Sources

Government and Institutional Resources

- Federal Bureau of Investigation (FBI)
  - Infragard
- United States Secret Service (USSS)
  - Electronic Crimes Task Force
- Department of Homeland Security (DHS)
  - United States Computer Emergency Readiness Team (US-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Financial Crimes Enforcement Network (FinCEN)
- Common Vulnerability Enumeration Database (CVE)
- National Vulnerability Database

Sector, Industry and Technology-Focused Resources

- Financial Services-Information Sharing and Analysis Center (FS-ISAC)
- Competitors, partners, and financial industry associations
- Industry news sites, e.g. krebsonsecurity.com, bankinfosecurity.com
- Information security sector sites, e.g. Internet Storm Center, Open Threat Exchange (OTX), ATLAS
- Managed security service providers (MSSPs) – blogs and feeds

FFIEC Cyber Security

- Main Site: https://www.ffiec.gov/cybersecurity.htm
- Board/Senior Management Video: http://youtu.be/t1ZgWKjynXI
- Observations: https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf

For More Information

- FBI Alert: Fraudulent ACH Transfers
  http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm
- FDIC Special Alert: Fraudulent Electronic Funds Transfers
  http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html
- FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes
  http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html
- NACHA Bulletin: Corporate Account Takeovers
  http://www.nacha.org/docs/NACHA%20Operations%20Bulletin%20-%20Corporate%20Account%20Takeover%20-%20December%202,%202009.pdf

For More Information (cont'd)

- FFIEC IT Handbooks
  http://ithandbook.ffiec.gov
- FFIEC Cybersecurity Awareness Web Site
  http://ffiec.gov/cybersecurity.htm
- Financial Stability Oversight Council 2015 Annual Report
  http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2015-Annual-Report.aspx
- The FDIC's "Cyber Challenge: A Community Bank Cyber Exercise"
  http://www.fdic.gov/regulations/resources/director/technical/cyber/cyber/htm
- Financial Services-Information Sharing and Analysis Center (FS-ISAC) www.fsisac.com/
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov/
- InfraGard
  www.infragard.org/
- U.S. Secret Service Electronic Crimes Task Force www.secretservice.gov/ectf.shtml
- The Top Cyber Threat Intelligence Feeds
  www.thecyberthreat.com/cyber-threat-intelligence-feeds/

Questions