FFIEC Cybersecurity Assessment Tool

June 30, 2015
Agenda

- Risk Trends
- FFIEC Cybersecurity Efforts
- Cybersecurity Assessment Tool
Cyber Risk Trends
Risk 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
Risk Trends

- **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.
Potential Impacts

- Financial
- Operational
- Legal
- Reputational
FFIEC Cybersecurity Efforts
FFIEC Cybersecurity Efforts

- Cybersecurity and Critical Infrastructure Working Group
- Joint statements and alerts
- Cybersecurity awareness website and CEO webinar
- Cybersecurity assessment of community institutions
FFIEC Cybersecurity Efforts

- Issue a Cybersecurity Assessment Tool
- Enhance incident analysis
- Align, update and test crisis management protocols
- Develop training programs for staff
- Update and supplement the *Information Technology Examination Handbook*
- Enhance focus on Technology Service Providers
- Collaborate with law enforcement and intelligence agencies
FFIEC Cybersecurity Assessment Tool
Objective
To help institutions identify their risks and determine their cybersecurity maturity.

The Assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness.
Consistent with the principles in

- FFIEC Information Technology Examination Handbook (IT Handbook)
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Industry accepted cybersecurity practices
Consists of two parts

Part One: Inherent Risk Profile
Part Two: Cybersecurity Maturity
Inherent Risk Profile Categories

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats
Inherent Risk Profile Risk Levels

Type, volume, and complexity of operations and threats directed at the institution
## FFIEC Cybersecurity Assessment Tool

### Inherent Risk Profile Excerpt

<table>
<thead>
<tr>
<th>Category: Technologies and Connection Types</th>
<th>Risk Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of internet service provider (ISP) connections (including branch connections)</td>
<td>Least</td>
</tr>
<tr>
<td>No connections</td>
<td>Minimal complexity (1-20 connections)</td>
</tr>
<tr>
<td>Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)</td>
<td>None</td>
</tr>
</tbody>
</table>
Cybersecurity Maturity

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Response
FFIEC Cybersecurity Assessment Tool

Cybersecurity Maturity

Domains

Assessment Factors

Components

Declarative Statements
# FFIEC Cybersecurity Assessment Tool

<table>
<thead>
<tr>
<th>Domain</th>
<th>Assessment Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cyber Risk Management &amp; Oversight</td>
<td>• Governance</td>
</tr>
<tr>
<td></td>
<td>• Risk Management</td>
</tr>
<tr>
<td></td>
<td>• Resources</td>
</tr>
<tr>
<td></td>
<td>• Training and Culture</td>
</tr>
<tr>
<td>2 Threat Intelligence &amp; Collaboration</td>
<td>• Intelligence Sourcing</td>
</tr>
<tr>
<td></td>
<td>• Monitoring and Analyzing</td>
</tr>
<tr>
<td></td>
<td>• Information Sharing</td>
</tr>
<tr>
<td>3 Cybersecurity Controls</td>
<td>• Preventative Controls</td>
</tr>
<tr>
<td></td>
<td>• Detective Controls</td>
</tr>
<tr>
<td></td>
<td>• Corrective Controls</td>
</tr>
<tr>
<td>4 External Dependency Management</td>
<td>• Connections</td>
</tr>
<tr>
<td></td>
<td>• Relationships Management</td>
</tr>
<tr>
<td>5 Cyber Incident Management &amp; Resilience</td>
<td>• Incident Resilience Planning and Strategy</td>
</tr>
<tr>
<td></td>
<td>• Detection, Response and Mitigation</td>
</tr>
<tr>
<td></td>
<td>• Escalation and Reporting</td>
</tr>
</tbody>
</table>
FFIEC Cybersecurity Assessment Tool

Maturity Levels

- Innovative
- Advanced
- Intermediate
- Evolving
- Baseline
## Cybersecurity Maturity Excerpt

### Domain 1: Cyber Risk Management and Oversight

<table>
<thead>
<tr>
<th>Assessment Factor: Governance</th>
<th>Y, N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.</td>
</tr>
<tr>
<td></td>
<td>Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.</td>
</tr>
<tr>
<td></td>
<td>Management provides a written report on the overall status of the information security and business continuity programs with the board or an appropriate committee of the board at least annually.</td>
</tr>
<tr>
<td></td>
<td>Budgeting process includes information security related expenses and tools.</td>
</tr>
<tr>
<td></td>
<td>Management considers the risks posed by other critical infrastructures (e.g., telecom, energy) to the institution.</td>
</tr>
</tbody>
</table>
FFIEC Cybersecurity Assessment Tool

Inherent Risk Levels

Least  Minimal  Moderate  Significant  Most

Cybersecurity Maturity Level for Each Domain

Innovative
Advanced
Intermediate
Evolving
Baseline
Supporting Materials

- User’s Guide
- Overview for CEOs and Boards of Directors
- Appendix A: Mapping Baseline Statements to FFIEC IT Handbook
- Appendix B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework
- Appendix C: Glossary
Benefits to Institutions

- Identifying factors contributing to and determining the institution’s overall cyber risk.
- Assessing the institution’s cybersecurity preparedness.
- Evaluating whether the institution’s cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that could be enhanced and actions that could be taken to achieve the institution’s desired state of cyber preparedness.
- Informing risk management strategies.
Thank you