Cybersecurity Maturity Assessment: Are you where you should be?

NAFCU Services Webinar: 2/23/2016
Introduction

Matt Mitchell, CISSP- Director Risk Assurance

- 18 years information security experience
  - Security program definition and implementation
  - Risk and compliance management
  - Advanced threat simulation and detection

Knowledge Consulting Group

- A ManTech International Corporation company with over 900 cyber security professionals
- Pure-play cybersecurity solution provider
- Preferred Partner for NAFCU penetration testing and security advisory services
- Serves public & private sector customers
Agenda

- Introduction
- What is risk management
- Cyber risk management fundamentals
- Overview of the FFIEC Cybersecurity Assessment Tool (CAT)
- Putting the FFIEC CAT to work
- Analyzing the results
- Plan for improvement
- Q&A
What is Risk?

Simple Definition of Risk

1. The possibility that something bad or unpleasant (such as an injury or a loss) will happen.
2. Someone or something that may cause something bad or unpleasant to happen.
Risk decisions must be coupled with context and appetite

Context

• What is important to you?
• Information assets
• Reputation
• Members

Risk Appetite

• The amount and type of risk that an organization is willing to take in order to meet their objectives
What is Risk Management?

A *continuous* process designed to mitigate risk aligned with your risk appetite.
Cyber risk management fundamentals

1. What are you trying to protect
2. How are your assets used?
3. System or Application Architecture(s)
4. Threat Modeling
5. Define and implement countermeasures
6. Monitor capabilities

TRUSTED CYBER ADVISOR
Introducing the FFIEC Cybersecurity Assessment Tool

- Published in June 2015
- The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.
  - Identify an institution’s inherent risk relevant to cyber risks
  - Determine an institution’s current state of cybersecurity preparedness across cyber domains
- Incorporates cybersecurity-related principles from the FFIEC Information Technology (IT) Examination Handbook
- Designed to be a recurring analysis, not a one time event
Benefits

Provides a streamlined ability to enhance their oversight and capabilities of a credit union’s cybersecurity program

- 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 are needed or need enhancement and actions to be taken to achieve the desired state
- Informing risk management strategies
The cybersecurity assessment process

- Determine risk profile
- Assess cyber domain maturity levels
- Check alignment
- Plan for improvement

…and repeat…
Risk profile analysis

Establishing risk profile through qualitative risk analysis across 39 areas in six categories

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

Risk profile:
- Least
- Minimal
- Moderate
- Significant
- Most
## Determine your risk profile

Add up risk scoring to determine overall risk profile

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Least</th>
<th>Minimal</th>
<th>Moderate</th>
<th>Significant</th>
<th>Most</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technologies and Connection Types</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Delivery Channels</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online/Mobile Products and Technology Services</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Organizational Characteristics</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>External Threats</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>4</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>8</td>
</tr>
</tbody>
</table>
Cyber security domains & assessment factors

Domain 1: Cyber Risk Management & Oversight
- Governance
- Risk Management
- Resources
- Training and Culture

Domain 2: Threat Intelligence & Collaboration
- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls
- Preventative Controls
- Detective Controls
- Corrective Controls

Domain 4: External Dependency Management
- Connections
- Relationship Management

Domain 5: Cyber Incident Management and Resilience
- Incident Resilience Planning and Strategy
- Detection, Response, and Mitigation
- Escalation and Reporting
Similar to CMMI maturity model the FFIEC model has 5 levels

- **Baseline**: Minimum expectations required by law and regulations or recommended in supervisory guidance.
- **Evolving**: Detailed, formal processes. Controls are validated and consistent.
- **Intermediate**: Cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement.
- **Advanced**: Documented procedures and policies that are not already required. Risk-driven objectives are in place. Cybersecurity is formally assigned.
- **Innovative**: Driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks.
Determining cyber maturity

For each assessment factor analyze the declarative statements and select the maturity level in which all statements are met.

### Domain 1: Cyber Risk Management and Oversight

#### Assessment Factor: Governance

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Baseline</th>
<th>Evolving</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Y, N</td>
<td></td>
</tr>
</tbody>
</table>

**Baseline**
- 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. *(FFIEC Information Security Booklet, page 3)*
- Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 6)*
- Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. *(FFIEC Information Security Booklet, page 5)*
- The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)*
- Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *(FFIEC Business Continuity Planning Booklet, page J-12)*

**Evolving**
- At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.
- Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.
- Cybersecurity tools and staff are requested through the budget process.
- There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.
Maturity level may exceed the necessary risk mitigation resources, consider re-allocating to weaker areas or domains.

Improvements are required to strengthen cybersecurity to meet the higher risk profile.
Analyze, communicate, and develop a roadmap for improvement

- Compare maturity and risk levels across cybersecurity domains
- Identify if you are allocating focus and resources in the right areas based on your risk profile and appetite
- Communicate the results at all levels
- Have open and frank discussions about
  - Strengths
  - Weaknesses
  - Opportunities for improvement
  - Opportunities to reduce or transfer risk
- Make a cybersecurity capability plan and execute
Continuous evaluation
Expect, accept, and plan for change
Questions?

Matt Mitchell, CISSP
Director- Risk Assurance Services
Knowledge Consulting Group, a ManTech Company
2000 Edmund Halley Dr. Suite 500
Reston, VA 20191
Phone: 703-674-3845
Email: matthew.mitchell@mantech.com