VOL. 7 | October 26, 2015

INFORMATION TECHNOLOGY UPDATE

FFIEC Cybersecurity Assessment Tool – Another Risk Assessment?

In June of 2015, the FFIEC rolled out a Cybersecurity Assessment Tool designed to help institutions identify their risks and determine their cybersecurity maturity. While the content within this advisory is certainly not new material, the documentation requirements and format for banks is new. The FFIEC sites that their new assessment tool is consistent with the FFIEC Information Technology Examination Handbook (IT Handbook) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It has been speculated that regulators will begin looking at financial institutions' compliance with this new advisory as early as May of 2016.

The Assessment advises financial institutions to take part in two exercises: An Inherent Risk Profile and a Cybersecurity Maturity Level exercise. Both the Inherent Risk Profile and the Cybersecurity Maturity Levels are broken down into five parts/areas described at a high-level below:

Inherent Risk Profile

- Technologies and Connection Types
  - ISP (Internet Service Providers)
  - Third-party connections
  - Wireless
  - Volume of network traffic and devices
  - End-of-life systems
  - Cloud services
  - Personal devices
- Delivery Channels
  - Online availability
  - Mobile availability
  - ATM operations
- Online/Mobile Products and Technology Services
  - Payment services
  - P-2-P (person-to-person) payments
  - ACH
  - Wire transfers
  - Wholesale payments
  - Merchant remote deposit capture
  - Treasury services
  - Client and trust services
  - Global remittances
  - Correspondent banking
  - Merchant activity
- Organizational Characteristics
  - Recent mergers and acquisitions
  - Number of direct employees and contractors
  - Changes to security staffing
  - Privileged access
  - Changes in IT environment
  - Locations and business presence
  - Location of operations and data centers
- External Threats
  - Volume of attacks
  - Sophistication of attacks

2100 Corporate Drive, Suite 400 Wexford, PA 15090 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800

Cybersecurity Maturity Levels

- Cyber Risk Management and Oversight
  - Governance
  - Risk management
  - Resources
  - Training and culture
- Threat Intelligence and Collaboration
  - Threat intelligence
  - Monitoring and analyzing
  - Information sharing
- Cybersecurity Controls
  - Preventative controls
  - Detective controls
  - Corrective controls
- External Dependency Management
  - Connections
  - Relationship management
- Cyber Incident Management and Resilience
  - Incident resilience planning and strategy
  - Detection, response, and mitigation
  - Escalation and reporting

The Inherent Risk Profile is conducted without consideration for controls in place to mitigate risk. Instead, its purpose is to determine the financial institution's risk based solely on technologies and environmental factors without considering controls that have already been established to reduce the level of risk. The Cybersecurity Maturity Level is then determined by factoring in those controls that are in place to mitigate risk and determining the institution's actual maturity level.

Once completed, management and the Board of Directors should review the current maturity level to determine if they are comfortable with the maturity level based on the inherent risk. If not, they are encouraged to continue the process of improving their security posture by doing the following:

- Determining a target maturity level (where the institution would like to be)
- Performing a gap analysis (determining gaps and requirements to achieve the target level)
- Prioritizing and planning (itemizing what needs to be done in what order to achieve the target level)
- Implementing changes
- Re-evaluating (determining whether the target maturity level was achieved)
- Communicating results to the Board of Directors

At the surface, the above guidance appears to be yet another risk assessment to be performed by financial institutions. While the assessment tools do resemble a risk assessment, the requirement to establish and meet a target risk maturity, or risk appetite, is new. This new standard will require financial institutions to continually monitor and document their cybersecurity maturity level and determine if gaps exist between the current and target level. Thus, as new threats and new technologies are introduced, this tool/assessment would be revisited to determine how those new items are affecting the institution's cybersecurity maturity model.

Questions?

If you have any questions regarding this document or the resources listed below, please feel free to contact Jeremy Burris, Rob Haller, or Chris Kreutzer at (724) 934-0344 or (800) 580-7738, or email jburris@srsnodgrass.com, rhaller@srsnodgrass.com, or ckreutzer@srsnodgrass.com.

References/Resources

The FFIEC has provided the original guidance along with several supplements, which include recommended resources for conducting the Inherent Risk Profile and the Cybersecurity Maturity Level exercise. These can be found using these hyperlinks:

Original Guidance on Cybersecurity Assessment Tool
Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook
Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework
Inherent Risk Profile Worksheet
Cybersecurity Maturity Model