Cybersecurity

August 10, 2022

Moderator: **Charlie Clark**, Director, Washington Department of Financial Institutions

Panelists: **Tom Fite**, Commissioner, Indiana Department of Financial Institutions, CSBS Chair

Rick Hill, Vice President of Industry Technology, Mortgage Bankers Association

Brad Robinson, Senior Director Cybersecurity Policy and Supervision, CSBS

American Association of Residential Mortgage Regulators

Cybersecurity Resources

- MBA Basic Components of an Information Security Program
  - https://www.mba.org/industry-resources/technology-resource-center/cybersecurity
- FFIEC Cybersecurity Assessment Tool
  - https://www.ffiec.gov/cyberassessmenttool.htm
- NIST Cybersecurity Framework
  - https://www.nist.gov/cyberframework/framework
- CSBS Nonbank Cybersecurity Assessment Program – Link TBD

MBA Basic Components of an Information Security Program

- Manage Risk
- Protect your Endpoints
- Protect Your Internet Connection
- Patch Your Operating Systems and Applications
- Make Backup Copies of Important Business Data/Information
- Control Physical Access to Your Computers and Network Components
- Secure Your Wireless Access Points and Networks
- Train Your Employees in Basic Security Principles
- Require Individual User Accounts for Each Employee on Business Computers and for Business Applications
- Data Management
- Limit Authority to Install Software
- Create Business Policies Related to Information Security
- Exercise Due Diligence in Hiring Employees
- Get Help With Information Security When You Need It
- Perform an Asset Inventory (and Identify Sensitive Business Information)
- Implement Encryption to Protect Your Business Information
- Third Party Risk Management
- Plan for Business Continuity and Disaster Recovery
- Software Development Life Cycle (SDLC) / Change Control

American Association of Residential Mortgage Regulators

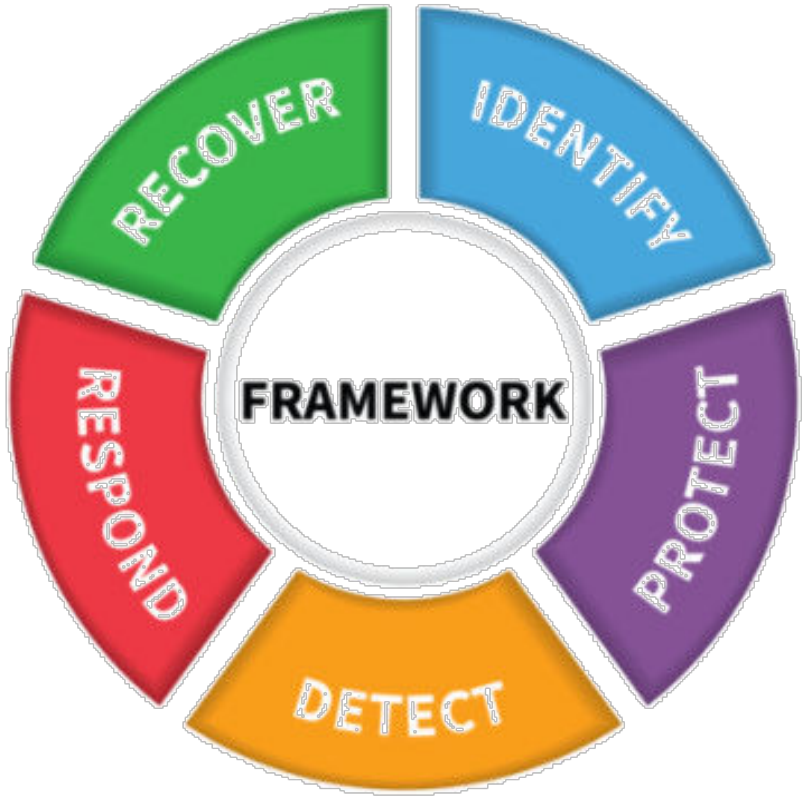
FFIEC Inherent Risk Profile

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed

FFIEC Cybersecurity Maturity

IT ASSET MANAGEMENT	**Baseline**		An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. *(FFIEC Information Security Booklet, page 9)* Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. *(FFIEC Information Security Booklet, page 12)* Management assigns accountability for maintaining an inventory of organizational assets. *(FFIEC Information Security Booklet, page 9)* A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. *(FFIEC Information Security Booklet, page 56)*
	Evolving		The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets. The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards. The institution proactively manages system EOL (e.g., replacement) to limit security risks. Changes are formally approved by an individual or committee with appropriate authority and with separation of duties.

NIST Cybersecurity Framework



- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

American Association of Residential Mortgage Regulators