CYBERTALK

MANAGING A COMPLEX TOPIC

Cybersecurity is a technical topic, and bank management often find it difficult to communicate with executives and boards of directors on this subject. This Cyber Talk series provides helpful hints on how management can explain the bank's cybersecurity posture to its board and implement a cybersecurity framework across its IT estate.

ANSWERING THE QUESTION

So how does bank management answer the question, "How are we doing on cybersecurity?" The answer: Implement a technical control framework across the bank and report on its level of penetration across the bank's IT estate. When executives and the board understand the goal is the framework, then they better understand the path being taken to get there.

How to Implement Cybersecurity Frameworks

1) Identify the right framework for your institution.

- Consider the resources that are available to the bank to use for framework implementation.
- Consider the current maturity level of the IT security program.
- Interview staff on their knowledge-base of frameworks and identify their level of understanding in this space.
- Consider the training resources that would be necessary depending on the framework that is chosen.

2) Educate executive staff and the Board of Directors.

- Executive staff and the board need to understand the value of the framework once it is implemented.
- Realistic expectations on frame-work implementation will facilitate a better digestion of the reporting that will follow the control gap analysis.

3) Perform the technical control gap analysis.

- Perform an assessment of the cybersecurity controls currently in place across the IT estate.
- Compare the identified controls against those listed in the chosen framework.
- Determine whether your institution meets the requirements of "basic cyber hygiene." If it does not, work on those controls first as they represent the most critical aspect of the cybersecurity program.

4) Fill the identified technical control gaps.

- Formulate an Information Security Strategy and identify the projects necessary to increase the cybersecurity posture of the institution.
- Draft project plans that directly satisfy the controls noted within the chosen framework.
- Determine the resources (staff hours and capital spend) needed to execute the project plans and educate the board on how this plan will improve the bank's cybersecurity posture.

5) Report on implementation success.

- In a report, identify the controls that the bank is moving forward to implement in its current phase.
- Correlate the capital spend to each of the critical controls and visually report on the increase in the cybersecurity posture as the controls are implemented and the bank begins to satisfy basic cyber hygiene.

This process is not going to be completed overnight, and will likely be a multi-phased, multi-year set of projects. Like all things in IT, the framework should be adaptable to the changing technologies and services of the bank and future projects should consider framework requirements.

FEDERAL RESERVE BANK of ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

Baseline - A documented version of a hardware component, software program, configuration, standard, procedure, or project management plan. Baseline versions are placed under formal change controls and should not be modified unless the changes are approved and documented.

Center for Internet Security® (CIS®) - Non-profit entity whose mission is to identify, develop, validate, promote, and sustain best practice solutions for cyber defense and to build and lead communities to enable an environment of trust in cyberspace. The CIS now oversees and maintains the Top 20 Critical Security Controls framework that was historically developed by the SANS Institute.

Chief Information Security Officer (CISO) - A senior-level executive responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats.

Cybersecurity Framework - A tool to help organizations better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it fosters risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Cyber Hygiene - A foundational set of six security controls that form a strong defense against a multitude of IT-related attack vectors. Basic cyber hygiene challenges administrators to answer these five questions: What is connected to the network? What software is running on the network? Are you managing your systems? Are you looking for known bad software? Do you track those with administrative privileges?

Cybersecurity Posture - Security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Fintech – Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.

Framework - A structure around or over which something is built.

Gap Analysis - A technique that a business uses to determine what steps need to be taken in order to move from its current state to its desired future state.

IT Estate - All components of an organization's IT program regardless of the geographic location or logical separation.

Managed Security Service Provider (MSSP) - An IT service provider that provides an organization with some amount of cybersecurity monitoring and management, which may include virus and spam blocking, intrusion detection, firewalls and virtual private network (VPN) management.

National Institute of Standards and Technology (NIST) - The National Institute of Standards and Technology is a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce. NIST is the primary author of the NIST Cybersecurity Framework (CSF).

NIST Cybersecurity Framework (CSF) - A framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk. The CSF was developed by referencing a number of other industry standard frameworks.