economymatters

ANNUAL REPORT

ECONOMIC RESEARCH

BANKING & FINANCE

REGIONAL ECONOMICS

COMM/ECON DEV

INSIDE THE FED

DEPARTMENTS

Financial Tips
Podcast
Quizzes
Staff & Credits

Subscribe to e-mail updates

BANKING & FINANCE

(Less) Risky Business: An Overview of a New Cybersecurity Assessment Tool

October 15, 2015

Cybersecurity is a high-risk concern for the financial industry and supervisors. Since the 2012 distributed denial of service attacks, institutions have placed an even greater emphasis on improving security and combating potential incidents. Firms have increased their information technology (IT) security budgets and invested in systems and personnel to address these risks. Despite these efforts, institutions are unsure whether their actions are sufficient and are still seeking a comfort level with their preparations and ongoing security programs.

The Federal Financial Institutions Examination Council (FFIEC) members have also experienced challenges in assessing whether institutions' actions are appropriate and sufficient. To assist in answering these questions, the FFIEC has developed a cybersecurity assessment tool (CAT). This tool is designed to help financial institutions determine their inherent level of cybersecurity risk and then assess the appropriateness of their cybersecurity control environments given their identified risks. The FFIEC tool is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and existing regulatory guidance. It is not a silver bullet to address all cybersecurity concerns. However, it should help firms identify controls gaps in their environment based on their inherent risk profiles.

Implementation

On July 2, the Board of Governors issued SR letter 15-9 (FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors). The letter includes information on the CAT. Beginning in late 2015 or early 2016, the Federal Reserve plans to use these types of self-assessments in the review of cybersecurity preparedness in IT and safety and soundness examinations and inspections. Financial institutions and the industry will have the opportunity to provide feedback on the

assessment tool. Based on comments received, the FFIEC agencies will determine whether the assessment tool should be modified. The Federal Reserve is particularly intent on working with the other agencies to tailor supervisory expectations for financial institutions with low cybersecurity risk characteristics. As appropriate, additional supervisory expectations may be implemented for financial institutions with significant cybersecurity risk.

Establishing an inherent risk profile

The first portion of the CAT process focuses on the institution's current inherent risk environment. The tool helps determine the level of cybersecurity risk based on the firm's activities, services, and products. The inherent risk categories measured in the CAT include:

- technologies and connection type
- delivery channels
- online/mobile products and technology services
- organization characteristics and
- external threats

The assessment begins with measuring the inherent risk of technologies and connections. Certain connections may pose additional cyberrisks. The risk profile may be adjusted depending on the number of internet service providers and third-party connections and whether they are in-house or outsourced. The volume of unsecured connections and the use of end-of-life systems, cloud services, and personal devices can also increase the risk at a firm.

The second considered factor is the number and variety of delivery channels. The greater the number of online and mobile delivery channels and the use of smart ATMs, the greater the risks. Expanding the number of delivery channels also presents additional cyberthreat vectors. A financial institution's mobile or online services may also heighten risk, particularly if there is a funds transfer component.

Organizational changes can also raise the inherent cybersecurity risk at a firm. There have been instances in the past in which data breaches occurred after a merger as a result of a lack of control over the newly consolidated environment. In the postmerger environment, compiling a comprehensive inventory of hardware can be challenging. An overlooked server can go without security updates for a significant amount of time, which opens the door to a data breach. Also, in a postmerger environment, changes in staffing or the use of contractors can lead to excessive user-access privileges being granted and then overlooked. Lastly, organizational changes can also affect morale, which may increase the potential of an insider security threat.

The last inherent risk factor comes from external threats. A large multinational financial institution will have a higher risk profile than a small community bank in a rural setting. Both firms will always face the potential for a cyberattack. However, the small community bank may be unknown outside of its market area and face fewer threats.

Considering cybersecurity maturity

The second portion of the CAT focuses on assessing the cybersecurity maturity of a firm's control environment. The maturity levels are defined as:

- baseline
- evolving
- intermediate
- advanced and
- innovative

The baseline maturity level means that a firm is in compliance with regulatory guidance. An evolving firm is characterized by additional formalities of documented procedures and policies that exceed regulatory requirements. An institution with an intermediate state of maturity has a detailed, formal process in place where controls are consistent and validated. In a firm with advanced cybersecurity maturity, cybersecurity practices and analytics are integrated across all lines of business. A firm at the innovative level of maturity demonstrates innovation in people, processes, and technology in its management of cybersecurity risk. These firms are at the leading edge in developing and implementing new controls, tools, and information-sharing groups to address cyberrisk.

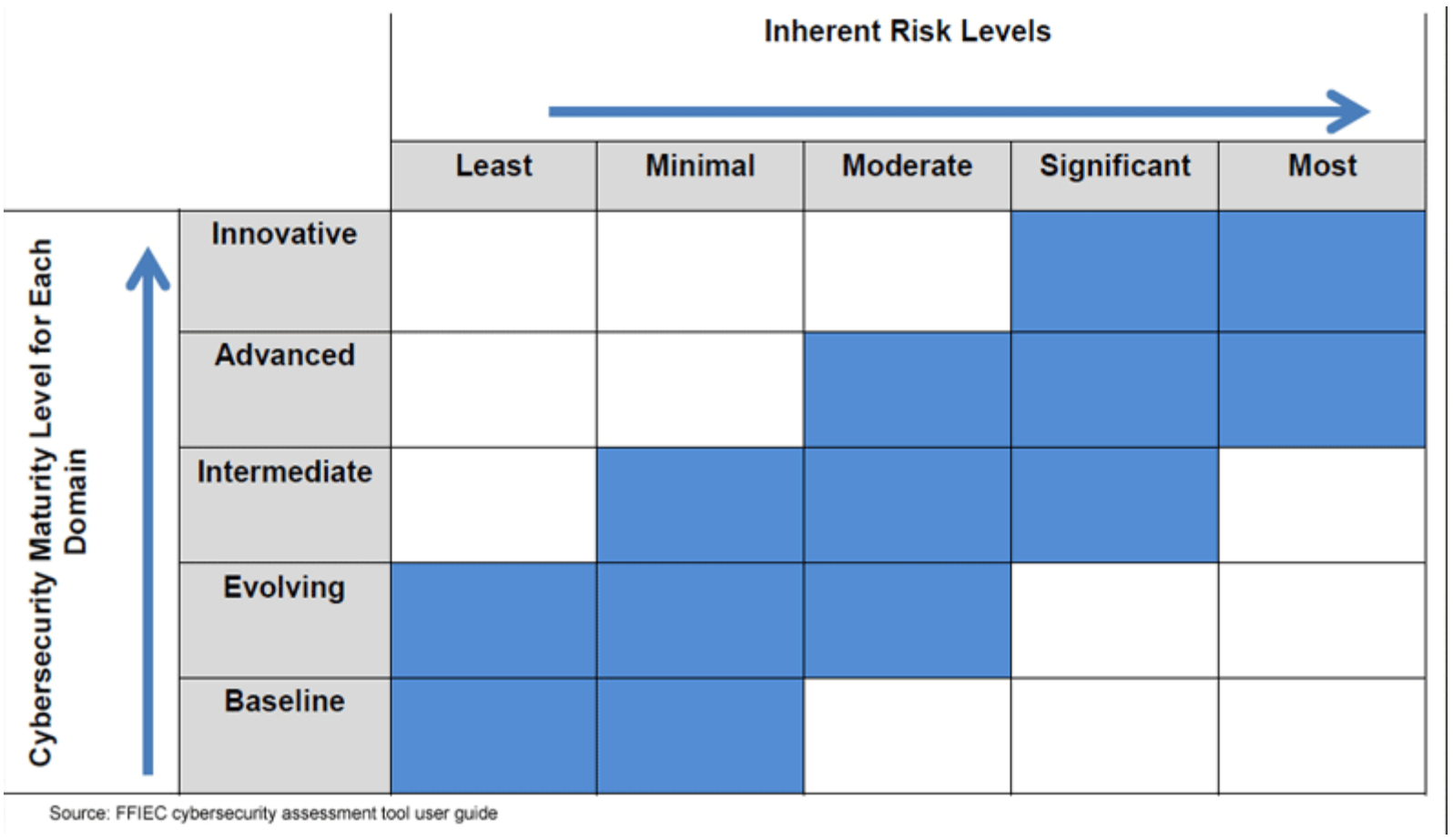
The maturity assessment also includes the following domains, for which cybersecurity maturity is measured. These domains include:

- cyberrisk management and oversight
- threat intelligence and collaboration
- cybersecurity controls
- external dependency management and
- cyberincident management and resilience

Cyberrisk management and oversight is the governance infrastructure that a firm has in place to oversee cyberrisk. Threat intelligence is the capability to monitor, acquire, analyze, and track the potential cyberthreat landscape and how it might affect the firm. Cybersecurity controls are the measures in place to deter and prevent a cyberattack. External dependency management relates to how well a firm manages its vendors and includes an assessment of the robustness of its vendor management program. The last domain is cyberincident management and resiliency, which concerns the steps management takes to identify, prioritize, respond to, and mitigate cyberthreats and vulnerabilities when they occur.

Using the CAT

The CAT provides management and boards of directors with a repeatable and measurable process to determine whether firms are applying sufficient resources and have the appropriate controls to manage cybersecurity risk. The CAT can help inform management and the board of their institution's level of inherent cyberrisk. The board may then consider this information and, given its risk appetite, determine the appropriate level of cybersecurity maturity needed to manage the firm's particular risk environment. Not all firms are expected to be at an innovative level of maturity. In fact, very few need to strive for this level. The chart below (taken from the FFIEC Cybersecurity Assessment Tool, June 2015, OMB Control 1557-0328) helps to define the appropriate levels of maturity based on the inherent cybersecurity risk identified.



Once the board determines the desired maturity level, management can then measure the current processes against this level, identify any gaps, and take action to move the firm's control environment toward the desired outcome.

Currently, the Fed examines many financial institutions and technology service providers in the southeastern United States. For these firms, hurricanes are a known risk. As a result, these institutions have very robust business continuity and disaster recovery plans. Plans are tested annually and are often activated because of weather events. Given this operating environment, these firms have learned to adapt quickly and resume operations with minimal impact on customers in the aftermath of a weather event. Financial institutions must reach this same level of maturity for managing cybersecurity risk. Firms should assume that it is only a matter of time before they experience a cyberevent. In the ideal state of maturity, when a cyberevent happens, firms will be prepared to react quickly, minimize impact, and resume operations as soon as possible. The CAT is a good first step toward moving the financial industry to this state of maturity.

In the future, the FFIEC will update the tool and the *IT Examination Handbook* based on the cybersecurity threat landscape. Additional information on the CAT and improving cybersecurity risk management is available.

By **Brian Bettle**, senior examiner in the Atlanta Fed's supervision and regulation division