A Framework for Cybersecurity

During the past decade, cybersecurity has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber attacks. In response, financial institutions and their service providers are continually challenged to assess and strengthen information security programs and refocus efforts and resources to address cybersecurity risks.

This article describes the evolving cyber threat landscape and the U.S. government's response to enhance the security and resilience of the nation's critical infrastructure sectors. The article discusses how components of financial institutions' information security programs, including corporate governance, security awareness training, and patch-management programs, should be enhanced to address cybersecurity risks, and concludes with an overview of actions taken by the federal banking agencies to respond to cyber threats.

The Evolving Threat Landscape

Historically, a bank's primary security concern centered on protecting physical data assets such as posted ledger cards, promissory notes, and critical documents in the vault as well as securing the perimeter of the bank premises. In today's banking environment, business functions and technologies are increasingly interconnected, requiring financial institutions to secure a greater number of access points. Innovation has resulted in greater use of automated core processing, document imaging, distributed computing, automated teller machines, networking technologies, electronic payments, online banking, mobile banking, and other emerging technologies. At the same time, physical data assets have been automated and a bank's sensitive customer information stored on computers has become as valuable as currency—a different kind of asset that needs safeguarding.

Cyber criminals use a variety of tactics. Some more common attack strategies in recent years include malicious software deployment, distributed denial-of-service (DDoS) attacks, and compound attacks.

Malware

Malicious software, commonly referred to as "malware," is a broad class of software generally used to gain access to or to damage a computer or system. Malware may infect a computer from a variety of access points. Perpetrators often include malware as an attachment to an email, or it is delivered from websites referenced in emails. The perpetrator tricks the email recipient into reading the email and opening the attachment or clicking on the link by crafting the email to look as though it came from a trusted source.

These emails that deliver the malware are often referred to as "phishing" emails as they are fishing for victims. A "spear phishing" email campaign is a subset of phishing in which the email content is tailored to the interests of a smaller group or a single recipient. Phishing and spear phishing campaigns mislead targets into providing sensitive information such as user names, passwords, credit card details, or personal sensitive information, such as date of birth and Social Security number, that can be used to commit identity theft against the individual or gain access to

A Framework for Cybersecurity

continued from pg. 3

bank systems for theft, disruption, or destruction.

Examples of malware include ransomware and wiper programs. "Ransomware" generally restricts all access to a computer and demands a ransom be paid for access to be restored. "Wiper" programs destroy data from the infected computer's hard drive and, in some cases, may be used to cover the attacker's tracks.

Distributed Denial-of-Service

A DDoS attack attempts to make a machine or network connected to the Internet unavailable to its intended users by overloading it with excessive Internet traffic. Given the nature of these attacks, DDoS attacks cannot be prevented, but they can be successfully mitigated. The ability to effectively manage a DDoS attack comes from the target's ability to control and recover from the attack, possibly by redirecting Internet traffic to a different server or engaging a DDoS mitigation service.

Compound Attacks

Another attack strategy is the use of "compound attacks," in which more than one method of attack is deployed simultaneously. For example, criminals have used DDoS attacks to distract a target organization while perpetrating another form of attack. Or a phishing email may contain an attachment or link that, if clicked by the target, downloads a seemingly harmless file that contains hidden malicious software with delayed execution commands.

As the banking industry necessarily innovates to take advantage of new technologies and delivery channels, it needs to be alert to any related new avenues of cyber attacks. Banks can help mitigate these attacks by developing an effective cybersecurity awareness campaign for employees and customers, a comprehensive patching program, and a strong detection program. A sound risk-management program and corresponding controls will help mitigate the threat of cyber attacks.

A Critical Infrastructure Perspective

On February 12, 2013, the President issued Executive Order 13636, "*Improving Critical Infrastructure Cybersecurity*," which established that "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The Executive Order directed the National Institute of Standards and Technology (NIST) to develop a risk-based cybersecurity framework to serve as a set of voluntary consensus standards and industry best practices to help organizations manage cybersecurity risks. The NIST[1] defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks."

The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[2] was created through collaboration

[1] NIST is a non-regulatory, federal agency within the U.S. Department of Commerce. See: www.nist.gov.

[2] The Framework for Improving Critical Infrastructure Cybersecurity can be found at: http://www.nist.gov/cyberframework/.

between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The first version of the cybersecurity framework was released on February 12, 2014, and consisted of five core areas: Identify, Protect, Detect, Respond, and Recover.

The cybersecurity definition and the components in the framework are similar to the concepts found in Appendix B to Part 364 of the FDIC's Rules and Regulations. Appendix B was established as a result of the enactment of the *Gramm-Leach-Bliley Act* in 1999 and required each financial institution to develop an information security program. Use of the cybersecurity framework is not intended to replace a bank's traditional information security program, but rather modify the program to address emerging cyber risks. A bank's information security program should evolve as the operating environment and the threat landscape change. An effective information security program is not static and should be regularly evaluated and updated.

Bank management must incorporate cybersecurity into the bank's overall risk-management framework; design and implement appropriate mitigating controls; update respective policies and procedures and, ultimately, validate the intended control structure through an audit program. When designing a cyber risk control structure, four components of traditional information security programs are critical: Corporate Governance, Threat Intelligence, Security Awareness Training, and Patch-Management Programs.

Corporate Governance of Cybersecurity

An institution's executive management and Board of Directors (board) play a key role in overseeing programs to protect data and technology assets and establishing a corporate culture consistent with the bank's risk tolerance. A bank should evaluate and manage cyber risk as it does any other business risk. It is not simply the obligation of those employees in the server room, but rather an enterprise-wide initiative involving all employees. It is critical the board institute a corporate culture prioritizing cybersecurity.

Threat Intelligence

The Federal Financial Institutions Examination Council (FFIEC) on November 3, 2014, issued "*Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*." The statement indicates that, "[f]inancial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly." Essentially, it states that each financial institution should have a program for gathering, analyzing, understanding, and sharing information about vulnerabilities and threats to arrive at "actionable intelligence." Actionable intelligence can be gathered from various public and private sources.

The FFIEC statement encouraged financial institutions to participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC)[3] as a source of threat intelligence.

[3] The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. See: www.fsisac.com.

A Framework for Cybersecurity

continued from pg. 5

FS-ISAC is a public-private partnership that operates as an information-sharing forum. It was established by a Presidential directive to facilitate the sharing of threat and vulnerability information among critical infrastructure sectors. FS-ISAC information includes analysis and mitigation strategies about a multitude of topics including, but not limited to, information security, physical security, business continuity and disaster recovery, fraud investigations, and payment system risk. FS-ISAC also provides additional services and membership benefits including participation in webinars, workshops, threat exercises, and assistance in creating information filters to ensure an institution is receiving the threat and intelligence information it needs without experiencing information overload. To obtain this assistance, an institution need only call FS-ISAC toll-free at (800) 464-0085. In addition, FS-ISAC has created a community bank working group and sends weekly cyber updates to community bank executives. These updates use layman's language to explain the most pertinent cyber events of the week and to provide strategies for making the information actionable.

Another source of cyber intelligence is the U.S. Computer Emergency Readiness Team (US-CERT). US-CERT is part of the Department of Homeland Security and is focused on information regarding current security issues, vulnerabilities, and exploits. In addition to alerts, which an institution can receive by subscribing at www.us-cert.gov, US-CERT offers publications, educational material, and some assistance with cyber threats.

Security Awareness Training

Even the best-designed security controls cannot fully protect a financial institution from one uninformed employee, contractor, or customer who unwittingly visits a malicious Web site, opens a malicious email attachment, or clicks on a malicious email link. Effective cybersecurity awareness programs should educate employees, contractors, and customers about the threat environment and encourage them to "*Think Before You Click*."

Cybersecurity awareness programs should highlight the importance of guarding against cyber risks across all business lines and functions. Employees from entry-level staff to the board should participate in mandatory cybersecurity awareness training, as one uninformed employee can be the bank's weakest link.

Security awareness training should be role-specific, as job functions require access to different systems and types of information with varying levels of sensitivity. Cyber attacks may be customized and targeted at employees with greater access to data or the ability to modify security settings or install new applications, or those with the ability to initiate or authorize the transfer of funds. For example, frequent targets include information security professionals, executives, comptrollers, and cashiers.

Cybersecurity awareness training should be available to bank personnel and contractors as well as bank customers, merchants, and other third parties, as they represent additional access points to a bank's data systems

and can be targets of cyber criminals. For example, corporate account takeovers are typically perpetrated by the theft of a customer's login credentials that are used to transfer money from compromised accounts.

Patch-Management Programs

The lack of an effective patch-management program has contributed significantly to the increase in the number of security incidents. Patches are software updates designed to fix known vulnerabilities or security weaknesses in applications and operating systems.

An effective patch-management program should include written policies and procedures to identify, prioritize, test, and apply patches in a timely manner. The first step is to create an asset inventory cataloging the systems requiring patch-management oversight. The asset inventory should capture all software and firmware, such as routers and firewall operating systems, which are subject to periodic patches from vendors.

An effective program also should use information received from threat intelligence sources that report on identified vulnerabilities. Bank management should be aware of products reaching or at the end-of-life or those no longer supported by a vendor. Management should also establish strategies to migrate from unsupported or obsolete systems and applications and, in the interim, implement strategies to mitigate any risk associated with the use of unsupported or obsolete products.

The board and senior management should require regular, standard reporting (metrics) on the status of the patch-management program, including reports that monitor the identification and installation of available patches. Independent audits and internal reviews should validate the effectiveness of patch-management programs.

Regulatory Response and Resources

The FDIC monitors cybersecurity issues on a regular basis through on-site bank examinations, regulatory reports, and intelligence reports. The Corporation continually evaluates its own supervisory policies for potential improvement and encourages practices to protect against threats at the banks it supervises. The FDIC has taken a number of steps to increase industry awareness of cyber risks and to provide practical tools to help mitigate the risk of cyber attack.

In the spring of 2014, the FDIC issued a press release urging institutions to actively utilize available resources to identify and help mitigate potential cyber-related risks. It is important for financial institutions of all sizes to be aware of the constantly emerging cyber threats and government-sponsored resources available to help identify these threats on a real-time basis. The press release contained a number of examples of free resources available to institutions and their website addresses.

In the summer of 2014, the FDIC developed and issued the "Cyber Challenge" exercise, a resource for community banks to use in assessing their preparedness for a cyber-related incident, through a series of videos and simulation exercises that depicted actual events experienced by institu-

A Framework for Cybersecurity

continued from pg. 7

tions. The Cyber Challenge exercise is available free to all institutions on the FDIC website, www.fdic.gov, under the Community Banking Initiative link.[4]

In the summer of 2015, the FDIC created a cybersecurity awareness training program for FDIC-supervised institutions, as well as FDIC supervision staff and management. These sessions were held in each of the FDIC's regional offices during August 2015. One banker stated that during his examination after the session, he found great benefit in discussing what both he and his examiner heard at the cyber awareness training the week before. The training program was followed by a teleconference in October 2015 to provide an overview of the program and to share commonly asked questions and answers.

Lastly, in November 2015, the FDIC added three additional video simulation exercises to Cyber Challenge as well as a Cybersecurity Awareness video that provides an overview of the threat environment and steps community financial institutions can take to be better prepared should a cyber-attack occur. These materials are available free on the FDIC website, www.fdic.gov, under the Community Banking Initiative link.

The FDIC has also participated in a number of other activities as a member of the Federal Financial Institutions Examination Committee or FFIEC. In June 2013, the FFIEC created the Cybersecurity and Critical Infrastructure Working Group (CCIWG). The CCIWG's first major undertaking was to work to determine how well banks, particularly community banks, manage cybersecurity and to assess banks' preparedness to mitigate cyber risks. The FFIEC members conducted a pilot cybersecurity assessment during 2014 at more than 500 community institutions to evaluate preparedness. The results were reflected in the FFIEC document, "*Cybersecurity Assessment General Observations*," which provided themes from the assessment and suggested questions for chief executive officers and boards of directors to consider when assessing institutions' cybersecurity preparedness.[5]

The CCIWG also reviewed all outstanding regulatory guidance to identify any gaps and, as a result, the FFIEC IT Examination Handbook and other relevant regulatory guidance are being updated to address cybersecurity concerns. The CCIWG publishes cybersecurity information at http://www.ffiec.gov/cybersecurity.htm. The chart below provides an overview of recently released supervisory guidance and other FDIC or FFIEC resources that bank management may find useful in addressing cybersecurity risks.

[4] https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html.

[5] The "FFIEC Cybersecurity Assessment General Observations" presents general observations from the Cybersecurity Assessment about the range of inherent risks and the varied risk management practices among financial institutions. See: http://www.ffiec.gov/press/pr110314.htm.

Regulatory Action/Resource	Summary
Cybersecurity Awareness Technical Assistance Videos	This video series titled Cybersecurity Awareness is designed to assist bank directors with understanding cybersecurity risks and related risk management programs and to elevate cybersecurity discussions from the server room to the board room. The first video covers the evolution of data security, defines cybersecurity, and reviews the current cybersecurity threat environment. The second video reviews the components of traditional information security programs and discusses how elements of the program should be refocused in the current cybersecurity threat environment. See https://www.fdic.gov/regulations/resources/director/technical/cybersecurity.html
Vendor Management Technical Assistance Video	This video titled Outsourcing Technology Services is designed to assist bank directors with understanding responsibilities for governing their institution's vendor risk management program. The components of a program include a risk assessment process, service provider selection, contract negotiation and evaluation, and an ongoing monitoring framework. The video also discusses business continuity planning and testing and resources to assist with establishing and maintaining a vendor risk management program. To be released in early 2016.
Cyber Challenge: A Community Bank Cyber Exercise	The FDIC's simulation exercise, Cyber Challenge, is designed to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions. Using seven unique scenarios, the Cyber Challenge helps start an important dialogue among bank management and staff about ways they address operational risk today and techniques they can use to mitigate this risk in the future. Cyber Challenge is not a regulatory requirement; it is a technical assistance tool designed to help assess operational readiness. See https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html
Corporate Governance Technical Assistance Video	This presentation reviews corporate governance principles that are vital to a director's role in setting the direction of the bank. It focuses on three areas: (1) the role of a bank director, the associated responsibilities, and the importance of independent decision making; (2) direction on the supervision of bank operations; and (3) guidance to help directors stay informed. See https://www.fdic.gov/regulations/resources/director/virtual/governance.html
Information Technology (IT) Technical Assistance Video	The IT video is designed to enhance bank directors' awareness of effective risk management practices. The video illustrates key IT governance programs, discusses select emerging and significant IT risks, and provides relevant questions to consider at the directorate level. By doing so, it provides a reasonable foundation for bank directors to exercise their fiduciary oversight over ever-changing and challenging IT risks. See https://www.fdic.gov/regulations/resources/director/virtual/it.html

A Framework for Cybersecurity

continued from pg. 9

FFIEC Statement on Cyber Attacks Involving Extortion	This FFIEC statement, dated November 3, 2015, notified financial institutions of the increasing frequency and severity of cyber attacks involving extortion. It advised financial institutions to develop and implement effective programs to ensure the institutions are able to identify, protect, detect, respond to, and recover from these types of attacks. See http://www.ffiec.gov/press/PDF/FFIEC_Joint_Statement_Cyber_Attacks_Involving_Extortion_-_Interactive_Ve%20%20%20.pdf
FFIEC Cybersecurity Assessment Tool	On June 30, 2015, the FDIC, in coordination with the other FFIEC member agencies, issued the FFIEC Cybersecurity Assessment Tool to help institutions identify cybersecurity risks and determine their preparedness. Similar to a bank's information security program risk assessment, this voluntary tool provides management with a repeatable and measurable process to assess an institution's risks and cybersecurity preparedness. See http://www.ffiec.gov/cyberassessmenttool.htm
FFIEC Webinar: Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See	On May 7, 2014, the FFIEC's CCIWG hosted a Webinar entitled, Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See. The webinar was intended to raise awareness about the pervasiveness of cyber threats, discuss the role of executive leadership in managing these risks, and to share actions being taken by the FFIEC. See https://www.youtube.com/watch?v=t1ZgWKjynXI&feature=youtu.be
FFIEC Statement on Destructive Malware	This FFIEC statement, dated March 30, 2015, notified financial institutions of the increasing threat of cyber attacks involving destructive malware. It warned that financial institutions and technology service providers should enhance information security programs to ensure they are able to identify, mitigate, and respond to this type of attack. In addition, the statement recommended that business continuity planning and testing activities incorporate response and recovery capabilities and test resilience against cyber attacks involving destructive malware. See http://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf
FFIEC Statement on Cyber Attacks Compromising Credentials	This FFIEC statement, dated March 30, 2015, notified financial institutions of the growing trend of cyber attacks for the purpose of obtaining online credentials for theft, fraud, or business disruption and to recommend risk mitigation techniques. It said financial institutions should address this threat by reviewing their risk management practices and controls over information technology (IT) networks and authentication, authorization, fraud detection, and response management systems and processes. See http://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
Appendix J to the Business Continuity Planning IT Booklet: Strengthening the Resilience of Outsourced Technology Services	On February 6, 2015, the FFIEC issued an update (Appendix J) to the Business Continuity Planning IT Booklet entitled "Strengthening the Resilience of Outsourced Technology Services." This update stresses the importance of addressing and incorporating cybersecurity elements when establishing and monitoring third-party relationships. See http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

FFIEC Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing	This statement, dated November 3, 2014, indicated that financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly. It stated that each financial institution should have programs for gathering cyber-related information about vulnerabilities and threats in a timely manner, analyzing the data, and sharing information to arrive at "actionable intelligence." The statement also encouraged financial institutions to participate in the FS-ISAC as a source of threat intelligence. FS-ISAC information includes analysis and solutions about a multitude of topics including, but not limited to, information security, physical security, business continuity and disaster recovery, fraud investigations, and payment system risk. See http://www.ffiec.gov/press/pr110314.htm

Conclusion

Cyber risk is a substantial business risk. A bank's board and senior management must understand the seriousness of the threat environment and create a cybersecurity culture throughout the organization. The effective identification and mitigation of cyber risk must be grounded in a strong governance structure with the full support of the board and senior management.

Michael B. Benardo
Chief, Cyber Fraud and Financial Crimes Section
Division of Risk Management Supervision
mbenardo@fdic.gov

Kathryn M. Weatherby
Examination Specialist (Fraud)
Cyber Fraud and Financial Crimes Section
Division of Risk Management Supervision
kweatherby@fdic.gov