NELSON MULLINS

Safeguarding Your Financial Institution against Cyber Breaches
By David F. Katz

This article originally appeared in the American Bankers Association's Bank Compliance January 2016

Recent cyber attacks against financial institutions have compromised the personal information of millions of people and have underscored how cyber breaches are becoming a continual presence rather than a random occurrence. Over the last several years, financial institutions have increasingly become a primary target of foreign and domestic cyberattacks, identify theft, consumer financial fraud and other criminal activity. Even your institution's Non-Public Personal Information (NPPI) could have been impacted. That means it is no longer appropriate or advisable for an organization to adopt a reactive approach to their initiatives, as the consequences can be irreparable and very costly.

Rather when it comes to cyber attacks, the best offense is a proactive defense. But where should your organization start?

1. Strongly consider measures in light of past guidance and more recent guidance, and recommendations from regulatory authorities;
2. Financial institutions should review and reconsider their current incident response plans; and
3. Re-vamp the necessary steps that should be considered when developing and implementing these programs.

The focus of this article is on the emerging risks and Federal efforts, but several states are also trying to address the issue and you'll want to make sure your institution addresses state requirements as well.

Overview of Guidance from the Federal Financial Institutions and Examination Council (FFIEC)

The FFIEC has a well-established history of providing specific guidance to financial institutions in the area of cybersecurity. Most recently, in June 2015, the FFIEC released its initial version of the Cyber Security Assessment Tool (the Assessment) (www.ffiec.gov/press/pr063015.htm) to help financial institutions identify their risk and assess cybersecurity preparedness. The issuance of the Assessment was, in part, intended to be a follow up to the FFIEC's 2014 survey of 500 financial institutions.

The Assessment was developed in two parts: part one was designed to determine a financial institution's Inherent Risk Profile related to its formalized and implemented controls, and part two determines the current state of the cybersecurity program of the institution (referred to as "Maturity" by the FFIEC). The combined results indicate a financial institution's current state of cybersecurity preparedness, represented by maturity levels across five individual domains. The content of the Assessment is consistent with the principles of the FFIEC Information Technology Examination Handbook, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

As background, in 2012, the National Institute of Standards and Technology (NIST) published its Computer Security Incident Handling Guide, aimed at providing more detailed guidelines for incident handling. The FFIEC has neatly mapped the Assessment Tool to the NIST standards as well as industry-accepted cybersecurity practices. The FFIEC has also published resources to help financial institutions improve cybersecurity, including additional information regarding the cybersecurity assessment conducted in 2014. Finally, as far back as 2005, the FFIEC issued guidance to assist financial institutions in the development of in-house procedures that would serve to streamline an institution's response to a cybersecurity or data breach. This guidance was published in the form of Financial Institution Letters (FILs) and addressed to the CEOs of FDIC-supervised financial institutions.

In short, there is no shortage of published regulatory guidance for financial institutions in this area. However, each institution must apply the guidance and tools to its unique profile and circumstances.

As a threshold for consideration, the earlier 2005 guidance interprets Section 501(b) of the Gramm-Leach Bliley Act (GLBA), as well as the Interagency Guidelines Establishing Information Security Standards and stipulates that "financial institutions should develop and implement a response program to address incidents of unauthorized access to nonpublic personal information maintained by the financial institution or its service provider."

To summarize, in light of (1) the recent attention and continuing sophisticated guidance communicated by the FFIEC; (2) the recently announced tools available to conduct detailed risk assessments; and (3) the increasing threat, it is critical for institutions to carefully evaluate and update existing plans and processes around data governance and data security of NPPI.

In the event of a data breach or security incident, the FFIEC's recommended procedures call for an assessment of the nature and scope of the incident, followed by an immediate notification to the primary federal regulator. Additionally, the financial institution must file a Suspicious Activity Report (SAR) and notify law enforcement authorities where criminal investigations are ongoing.

But swift notice to regulators is not the only concern. Remember your Management 101 principles: First, stop the leak; then begin the clean-up. Financial institutions must also take steps to control the incident, prevent further unauthorized access to or use of customer information, and notify customers in a clear and conspicuous manner. Specifically, the financial institution must provide a description of the incident, the type of information exposed to such unauthorized access and the measures taken by the institution to protect customers from further exposure. The required customer notice must provide a telephone number that customers can call for information and assistance.

Key Elements of Incident Response

Appropriate response to information security incidents, including unauthorized access to NPPI, is a required component for compliance with section 501(b) of the GLBA. Each institution's Incident Response Plan should identify and prioritize security-related incidents, define appropriate responses to

incidents, such as the manner of investigation and the engagement of external advisors, and establish incident reporting requirements.

Once a plan is in place, it is the institution's responsibility to train its employees to execute the plan. Don't forget to make sure the Board and Management Team are up to speed. The sooner you can review, implement a plan and engage your team, the better.

Based upon the way the guidance is set-up, it's clear that the FFIEC is providing a subtle reminder of the way to manage this effectively, and other programs. Here are the eight key elements identified by the FFIEC for an effective and systematic Security Incident Response Plan:

1. Designate a Leader and Assemble a Team. First, an officer should be appointed who is responsible for determining whether a suspected event warrants full Incident Response Plan activation. In addition, this officer will be tasked with forming an incident response team responsible for the ongoing maintenance of the plan. This group includes the first responders to a security incident. Their mission is not only to prevent a serious loss of profits, public confidence, or information assets, but also to provide an immediate, effective and skillful response to any security incident. Perhaps it goes without saying, but the officer appointed to this role should have demonstrated capability and knowledge in the Security Incident Response space.

The appointed members of the incident response team should—at the very least—include individuals from executive and risk management, human resources, information technology, facilities/security, legal, internal communications/media relations, retail banking, bank operations, information security, and business continuity planning. The incident response team must determine when third-party, external advisors may be required to assist in responding, depending on the severity and nature of the incident. Such external advisors may include public relations, outside legal counsel, cyber forensics, cyber insurance brokers or FDIC regulatory professionals.

2. Prepare, Detect, and Analyze. Incident response is a steady-state, continuous process. Certain key actions should be taken before an incident occurs including: (1) establishing and maintaining corporate information security incident response standards and procedures; (2) planning and conducting security awareness sessions with team members and employees as well as security training, including continuing education for security operations; (3) preparing and maintaining a technical procedures and incident handling handbook for security operations and incident handlers; and (4) auditing, validating and reviewing security controls that are in-place and operational.

In addition, all employees and relevant external parties are required to enforce and adhere to all company information security policies, standards and procedures, and report potential violations to management. IT Security Operations should continuously monitor information systems for information security-related events. Technical controls must be deployed and maintained according to company standards to provide advance in-depth detection capabilities across all information systems.

3. Declare/Classify the Incident and Perform Triage. All potential security incidents should be immediately reported to the appropriate company post, such as the IT Help Desk. The Help Desk should

log the incident, gather incident-specific details and notify the incident response team right away for verification.

Some of the critical questions that need to be answered immediately are:
(1) Has the situation been remediated/neutralized or is the threat continuing?;
(2) What information or assets may have been compromised?; and
(3) What is the size, type and possible impact or exposure?

Based on all of the known information pertaining to the event, the information security team should determine whether or not to declare an official Information Security Incident.

When an incident has been declared, the team should perform triage by assessing the extent of compromise and damage. The incident response team will then make the decision as to whether it is necessary to notify law enforcement, regulators and any other authority. If necessary, the team will prepare a Suspicious Activity Report for filing through the established SAR process.

4. Determine Notification Requirements. Review the information gathered to determine if customer, consumer, NPPI or other confidential company information has been compromised. Has your bank's primary regulator been notified? Analyze appropriate state and federal laws and regulations to determine the likelihood that information has been or will be misused. It may be necessary to consult legal counsel in order to interpret current legislation with respect to customer notification requirements, review all contractual obligations, or to determine requirements to notify state and federal regulatory agencies or consumer reporting agencies.
If the security incident involves NPPI, it is likely that customers are required to be notified. Make sure that notices (when required) meet the requirements such as being clear and conspicuous, and you fully describe the incident and action taken, etc. And, be sure to include any additional information as dictated by the institution's policies. More information, when appropriate, should be included based on the nature of each security incident.

5. Investigate and Document the Incident. The initial step in this part of the plan is to determine whether or not the investigation should be conducted at the direction of the legal counsel to preserve attorney-client privilege. Collect, analyze, protect and preserve evidence as follows:

1. Institute a strict chain of custody;
2. Perform a forensically sound investigation;
3. Inventory the affected information systems and information assets compromised;
4. Document threat actor tactics, techniques and procedures observed; and
5. Report all findings to the incident response team.

The team should determine whether external forensic investigation services are required to respond to the security incident.

Event documentation is a critical aspect of incident response and investigation. From the early stages of incident response, companies shouldn't overlook the importance of documenting as much about a

security incident as possible, such as: dates and times of events, who or what system reported the event, all contact information, a detailed event description, identification of the asset and related event, and documentation of the customer notification exercise.

This information could be very valuable for law enforcement and with regard to post-incident review.

A helpful tool to organize and classify all incidents is an Information Security Incident Response Form, which should be easy to fill out and understand. This form should also include the most basic information regarding the incident, including primary responder contact information, an incident description highlighting discovery date/time, severity, attack technique and impact. Additionally, the form should document the measures taken to remediate and contain the incident, as well as what parties were notified.

6. Contain the Damage. The incident response team should take measures to contain and control the incident to prevent further unauthorized access to or use of non-public personal information by individuals. These measures might include modifying physical access controls, shutting down particular applications or third-party connections, reconfiguring firewalls, putting a hold on account information, securing paper documentation, changing computer access codes, and don't forget the staff training on any changes made.

Containment of an information security incident is vital. Containment methods are highly dependent on the type and scope of the incident. When possible and appropriate, certain steps should be followed to ensure a thorough and complete process, including preserving all system logs, audit logs, and evidence for law enforcement and potential criminal investigations, denying access to non-investigative personnel, restricting information about the incident to personnel on a need-to-know basis, and making sure that the Security Incident Response Form has been completed to memorialize and document the facts and containment measures made. Lastly, verify that the incident has been successfully contained.

7. Eradicate and Recover. Once the incident has been successfully contained, the financial institution must ensure that the same thing does not happen in the future. To do that, preventative measures must be implemented. All applicable passwords for information assets with access to NPPI need to be changed, and any and all compromised accounts should be immediately deactivated. Do not access or alter the compromised location of the information asset or shut down the compromised machine. Monitor information assets accessed for signs of continued intruder access, while also implementing firewall rules as needed to close any exposures identified during the investigation.

In addition, take appropriate steps to effectively eradicate the threat associated with the security incident. Eradication can be achieved by completely removing the cause(s) of the security incident. Remediate all vulnerabilities that may have contributed to the incident, and sweep all information systems for security-related indicators of compromise. Further, eliminate incident-related compromise indicators and other malicious artifacts from all information systems.

Once all necessary steps have been taken, verify that the eradication was successful, and then move to the recovery stage. Recover and restore information systems and information assets determined to have been compromised or implicated within the security incident.

8. Act Now. The sooner existing plans can be reviewed and updated, and you can engage your team, the better. A delay in either the adoption of an incident response plan or the implementation of strong controls, conducting a risk assessment and reprioritizing could be an expensive mistake. In light of past and present guidance from the FFIEC, it is prudent to constantly evaluate your financial institution's ability to remain strong in the face of a volatile cyber present and an uncertain cyber future.

Conclusion: It is likely that every financial institution will experience some type of security incident at some point. Since the vulnerabilities change almost daily, it is important that the institution's program is dynamic and responsive to trends and emerging risks. Periodic reviews and updates should be made to the program. Any thoughts such as "it can't (or won't) happen here" should be replaced by a dose of reality to the ever-changing cyber environment. No institution can afford to be complacent at any level when it comes to security incidents that too often cause compliance professionals to lose sleep.

ABOUT THE AUTHOR

David Katz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office where he leads the Privacy and Information Security Practice Group. He provides legal advice on matters related to the privacy laws affecting multiple sectors of the economy including retail, financial services, education, health care and technology. He counsels corporate clients on the development, management and oversight of privacy and compliance programs, vendor management programs and assists them in developing policies and procedures, education strategies, implementation of auditing and monitoring controls, reviews of disciplinary and enforcement activities, and risk assessments. His corporate practice includes providing privacy and security due diligence reviews for mergers and acquisitions. He represents client at all stages of incident response from investigation, notification, remediation and defense of litigation and regulatory inquiry. He may be reached at (404) 322-6122 or by email at david.katz@nelsonmullins.com. You may follow him on Twitter @KatzFDavid.

ENDNOTES

6. https://www.ffiec.gov/press/pr031715.htm. The conclusion of the survey report was as follows: *Today's financial institutions are critically dependent on IT to conduct business operations. This dependence, coupled with increasing sector interconnectedness and rapidly evolving cyber threats, reinforces the need for engagement by the board of directors and senior management, including understanding the institution's cybersecurity inherent risk; routinely discussing cybersecurity issues in meetings; monitoring and maintaining sufficient awareness of threats and vulnerabilities; establishing and maintaining a dynamic control environment; managing connections to third parties; and developing and testing business continuity and disaster recovery plans that incorporate cyber incident scenarios.*

2. The five domains which are the focus of the maturity level are as follows: Domain 1: Cyber Risk Management and Oversight. Domain 2: Threat Intelligence and Collaboration: Domain 3: Cybersecurity Controls: Domain 4: External Dependency Management: Domain 5: Cyber Incident Management and Resilience.

3. http://www.ffiec.gov/cybersecurity.htm.

4. Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, *Computer Security Incident Handling Guide*, Recommendation of the NIST, Special Publication 800-61, National Institute of Standards and Technology, U.S. Department of Commerce (August 2012), http://dx.doi.org/10.6028/NIST.SP.800-61r2

5. A mapping is available in Appendix B of the Cybersecurity Assessment Tool: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with cyber security framework principles and to highlight the complementary nature of the two resources.

6. FDIC Fin. Inst. Letter: Final Guidance on Response Programs, Guidance on Response Programs for Unauthorized Access to Customer Info. and Customer Notice, FIL-27-2005 (April 1, 2005) (on file with the FDIC Pub. Info. Ctr.).

7. The letters are typically used to announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to those responsible for operating a bank or savings association.

8. Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction that include administrative, technical, and physical safeguards, to protect the security and confidentiality of customer information.

9. 12 CFR 364, Appendix B.

10. FDIC Fin. Inst. Letter: Final Guidance on Response Programs, Guidance on Response Programs for Unauthorized Access to Customer Info. and Customer Notice, FIL-27-2005 (April 1, 2005) (on file with the FDIC Pub. Info. Ctr.).