Office of Inspector General

Executive Summary

The FDIC's Supervisory Approach to Cyberattack Risks

Report No. EVAL-15-003
March 2015

Why We Did The Evaluation

Information is one of a financial institution's (FI) most important assets. Protection of information is critical to establishing and maintaining trust between the FI and its customers, complying with laws and regulations, and protecting the FI's reputation. Most FIs rely heavily on information technology (IT) systems, external technology service providers (TSPs), and Internet-connected applications to provide or enable key banking functions. The importance of ensuring information security has grown and has become a vital component of operations as FIs and TSPs face growing challenges from cyberattacks.

A cyberattack is a deliberate exploitation of computer systems or networks. Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Our evaluation objectives were to assess the Federal Deposit Insurance Corporation's (FDIC) efforts to:

(1) Ensure that FI/TSPs are prepared to protect against, detect, respond to, and recover from cyberattacks;
(2) Provide sufficient and qualified resources to examine and monitor FIs and TSPs; and
(3) Promote information sharing about incidents to appropriate authorities.

Background

The FDIC conducts IT examinations of FDIC-supervised FIs and TSPs for compliance with sections 39 of the Federal Deposit Insurance Act (12 U.S.C. § 1831p-1) and 501(b) and 505(b) of the 1999 Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)). The federal banking agencies issued implementing *Interagency Guidelines Establishing Information Security Standards* (Interagency Guidelines) in 2001. In 2005, the FDIC developed the Information Technology—Risk Management Program (IT-RMP), based largely on the Interagency Guidelines, as a risk-based approach for conducting IT examinations at FDIC-supervised FIs. The FDIC generally conducts IT examinations of FIs in conjunction with risk management examinations.

The FDIC also uses work programs developed by the Federal Financial Institutions Examination Council (FFIEC) to conduct IT examinations of TSPs. The regulators perform comprehensive joint examinations of the largest TSPs and rotate examinations of mid-size TSPs. The FDIC's TSP examination and supervision authority originates from the Bank Service Company Act (12 U.S.C. § 1867(c)), which was enacted in 1962. The FDIC Chairman has recommended that Congress review the Act to ensure it adequately addresses third-party risk with respect to companies that provide direct services to FIs.

In February 2013, President Obama released Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which established policy to enhance the security and resilience of the Nation's critical infrastructure and called for the development of a risk-based cybersecurity framework and a program for its voluntary adoption. The National Institute of Standards and Technology released the *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014 to provide a blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of their computer systems.

Results

The FDIC's supervisory approach to cyberattack risks involves conducting IT examinations at FDIC-supervised FIs and their TSPs; staffing IT examinations with sufficient, technically qualified staff; sharing information about incidents and cyber risks with regulators and authorities; and providing guidance to institutions. The FDIC's IT examination program plays an important role in protecting the Nation's financial services infrastructure and ensuring that FIs and TSPs are prepared for cyberattacks. We concluded that the FDIC could increase the level of assurance that FIs and TSPs are adequately prepared by taking the following actions:

- Updating and expanding IT examination procedures,
- Providing consistency and transparency to IT examination scope and procedures performed,
- Ensuring that examiners consistently conclude on FI/TSP program level controls and consider the scope of vendors' third-party reviews,
- Completing efforts to estimate examiner resource and competency needs and ensuring those involved in reviewing IT examination reports receive sufficient and current training, and
- Continuing to enhance information sharing associated with cyber risks.

FDIC Primarily Relies on IT Examinations to Ensure FIs and TSPs Are Prepared for Cyberattacks

The FDIC's efforts to ensure that FIs and TSPs are prepared to protect against, detect, respond to, and recover from cyberattacks primarily involve conducting IT examinations. In 2013, the FDIC conducted 2,323 IT examinations at FIs and TSPs. The Division of Risk Management Supervision (RMS) periodically conducts IT examinations to assess FI/TSPs' information security programs and compliance with the Interagency Guidelines. In that regard, our evaluation showed that:

- The FDIC and FFIEC IT examination work programs focus on security controls at a broad program level that, if operating effectively, help institutions protect against and respond to cyberattacks. The program-level controls include risk assessment, information security, audit, business continuity, and vendor management. However, the work programs do not explicitly address cyberattack risk, could be updated and strengthened, and could better specify desired characteristics for key program-level controls. The FFIEC has an ongoing initiative to update its IT examination guidance to align with changing cybersecurity risks.

- Examiners review prior examination information and consider the technology profile of the FI in planning the scope of the examination. In addition, the IT-RMP is designed for examiners to rely, in part, on FI management attestations regarding the extent to which IT risks are being managed and controlled. Examiners focus their efforts on management-identified weaknesses and may confirm selected safeguards described by management as adequate. Examiners raised concerns about the value of FI management attestations, including whether the design of the attestation questionnaire provides meaningful information for scoping the examination.

- Examination reports routinely included a statement attesting to FI/TSPs' compliance with the Interagency Guidelines and frequently identified concerns or recommended improvements to information security programs. We determined that examiners frequently concluded on the adequacy of risk assessment and audit programs, but examiners were far less likely to have

documented their review and/or provided a clear statement of adequacy on intrusion detection programs and incident response plans. Because examiners have wide discretion in conducting and documenting IT examination work and are only required to document examination findings and recommendations, we could not always tell what procedures examiners performed to reach their conclusions.

- Examiner comments and our own review of examination working papers identified program weaknesses at a number of the FIs we sampled. For example, we noted variation in the quality and depth of FI risk assessments and other IT security program elements. With respect to vendor management, although FIs and the IT-RMP rely on periodic third-party reviews and audits of vendors' IT controls and risk management practices, we observed that vendors frequently obtained third-party reviews that provided lower levels of assurance. These reviews focused on internal control over financial reporting—versus reviews that address controls relevant to security, availability, processing integrity, confidentiality, and privacy.

FDIC's IT Examination Resource Needs and Competencies Depend Largely on Planned Examination Program Changes

The FDIC works to provide sufficient and qualified resources for IT examinations through its recruitment and training and development activities. We observed that the average hours spent conducting individual IT-RMP examinations has increased by about 21 percent since 2006. During 2013, RMS spent an average of 8-10 days to perform an IT examination at FIs with adequate or better IT security programs and 15-20 days for FIs exhibiting some degree of supervisory concern. The total number of IT examination staff[1] has increased by about 36 percent since 2008. However, much of the increase occurred in non-commissioned IT examination analyst positions, many of whom are term employees who will be leaving the FDIC soon. Moreover, some IT examination staff only spend a portion of their time conducting IT examinations.

RMS has training programs for developing IT examination staff which include mandatory and discretionary courses and Information Technology On-the-Job (IT-OJT) training experiences. While most IT examination staff have received IT training, many regional supervisors such as Assistant Regional Directors (ARD) and Case Managers have received limited IT examination training. ARDs and Case Managers are reviewing and approving reports of examination, which include the results of the IT examination. Accordingly, these officials would benefit from a continuing, basic foundation in IT examination principles and concepts, as well as knowledge of emerging environmental IT issues, trends, and risks within the banking industry.

We also observed a few situations where non-commissioned IT examination analysts conducted IT examinations of complex FIs under the supervision of a commissioned examiner who was not an IT specialist and situations where IT subject matter experts served as the examiner-in-charge on complex IT examinations before they completed required IT-OJT courses. These practices could present examination risk.

[1] For the purposes of this report, "IT examination staff" include IT risk management examiners, IT subject matter experts, regional office IT examination specialists, and IT examination analysts.

RMS conducted an IT examination workforce resource study in 2012 that found the utilization and development of examiners in the IT field had not kept pace with the FDIC's increased IT examination workload. The study concluded, in part, that more IT examination staff was needed and that IT training and development could be improved. The study included short- and long-term recommendations aimed to recruit examiners earlier in their career, train staff in the IT and operations risk management specialty area, and create a career map framework for specialty areas. With respect to training, the study proposed updating policies, funding to revitalize the core IT courses, and modifying who should attend IT-related courses. In response to the study, RMS noted that it has increased the number of IT subject matter expert positions and trained nearly 300 commissioned examiners to conduct less complex IT examinations. We concluded that determining future resource needs and examiner competencies will depend largely on whether and how the FDIC, together with the FFIEC, changes the approach to examining IT at FIs and TSPs.

FDIC has Ongoing Processes and Initiatives for Receiving and Sharing Cyberattack Information

The FDIC has processes for receiving cyber incident information and various initiatives to help promote information sharing about cyberattack incidents to FIs, the financial sector, and other regulators and authorities. The FDIC receives cybersecurity information through FI security incident reports and Suspicious Activity Reports filed with the Financial Crimes Enforcement Network. The FDIC participates in a number of interagency and financial sector councils and committees and will soon be approved to begin receiving classified intelligence information on cybersecurity incidents.

The FDIC periodically issues information security-related guidance to FIs on areas such as new regulations and policies. The frequency of FDIC-issued IT guidance increased markedly in 2014 and the FDIC's practice of issuing notices about specific industry cyber threats has evolved. For example, last year, the FDIC issued an alert advising FIs of a material security vulnerability associated with authenticating Internet services and encrypting sensitive information. The FDIC has also held webinars, issued technical assistance videos, and discussed cybersecurity issues with banking industry representatives.

The FDIC could enhance its information sharing activities by improving the categorization of specific types of cyberattacks in security incident reports and reaching agreements with other regulators to share security incident information.

OIG Recommendations, Corporation Comments, and Matters Warranting Further Study

The FDIC and the FFIEC have ongoing initiatives to update programs for examining FIs and TSPs. Accordingly, we framed our recommendations to complement RMS' efforts associated with updating examination and institution guidance, addressing resource and training challenges, and enhancing information collection and sharing initiatives.

The Director, RMS, responded to a draft of this report on March 6, 2015. RMS concurred with the report's nine recommendations and noted that RMS had started project plans for several of the recommendations. The response outlined corrective actions that were responsive to the

recommendations. RMS established planned completion dates for corrective actions throughout 2015 and 2016 and expects to have all actions completed by the end of 2016.

During our evaluation, several questions arose that were outside of the scope of our review. Given their varied nature, we may pursue some in more depth in separate reviews or in discussions with FDIC management. These questions include the consideration of how IT examination results could be further emphasized in safety and soundness ratings, challenges presented by differing IT examination cycles for FIs and TSPs, the sufficiency of contracts between FIs and TSPs, and the legal framework associated with addressing TSP weaknesses.