Office of Inspector General

Executive Summary

Case Study of a Computer Security Incident Involving a Technology Service Provider

Report No. EVAL-16-002
February 2016

Why We Did The Evaluation

In late 2014, we received allegations about a computer security incident potentially involving unauthorized access to unencrypted personally identifiable information (PII) from multiple client financial institutions (FI) residing on a technology service provider's (TSP) computer server. We initiated work to evaluate the TSP's and FDIC's handling of the matter with objectives to:

- Understand the specifics of the incident and assess the TSP's response and communications;
- Evaluate the FDIC's response to, and consideration of, the incident; and
- Evaluate the examination coverage of the TSP prior to the incident.

During our evaluation, we became aware of additional information that called into question the credibility of the allegations. Notwithstanding, this incident provided a real world example of challenges that the Corporation, TSPs, and FIs face when assessing and deciding how to respond to potential cyberattack issues. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Background

12 CFR Part 364, Appendix B, *Interagency Guidelines Establishing Information Security Standards*, requires FIs to implement a comprehensive written information security program designed to: ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. The Interagency Guidelines require FIs to develop and implement a risk-based response program to address incidents of unauthorized access to customer information. The Interagency Guidelines also provide that FIs' contractual arrangements shall require that TSPs implement appropriate measures to meet the Interagency Guidelines objectives. The federal banking agencies, including the FDIC, conduct periodic information technology (IT) examinations at FIs and their TSPs.

Evaluation Results

Following the incident, the TSP conducted an investigation and concluded that adware caused the suspicious activity and identified no evidence of a cyberattack or exfiltration of data. The TSP concluded that the incident did not warrant regulatory or client notification based on applicable regulatory guidance and client contract language. However, contrary to cybersecurity best practices, the TSP did not collect or retain forensics information such as an image of the server or a copy of the adware. Moreover, the TSP did not have computer activity logging controls in place that may have allowed the TSP to determine whether any data had been accessed or exfiltrated.

We concluded that a poor internal control environment and a vague incident response policy limited the TSP's ability to protect against the incident and hampered incident response efforts. We also concluded that the TSP could have done more to notify regulatory authorities of the incident and that the contract language between the TSP and its client FIs could have better defined terms related to incident response and specified notification requirements.

Once the FDIC's Risk Management Supervision (RMS) Washington Office became aware of the incident, it required the TSP to obtain a forensic investigation and deployed an examination team to review overall TSP network security. However, we concluded that the RMS field office could have escalated the security incident and allegations sooner. The incident demonstrated the importance of having an RMS incident response plan for assessing potentially significant cyber incidents and sufficient enforcement authority over TSPs.

With respect to examination coverage, while the FDIC led joint IT examinations in compliance with examination frequency requirements and implementing guidelines, we had several observations regarding the July 2014 IT examination related to the assigned rating and tone of the examination report, incident response coverage, consideration of third-party reviews, and work paper documentation.

Corporate Actions Taken

We made recommendations in a prior report to address several areas identified in this case study and RMS is working to implement those recommendations. RMS has also issued new guidance for escalating incidents; is developing a corporate plan for responding to significant cyber incidents; is researching whether to draft regulations to govern TSP operations, to include expectations for FI incident notifications; and has established several cyber-related performance initiatives. We plan to monitor RMS progress in completing these important actions. We also expect to perform further reviews in this area in light of the significant risks that technology services present to the financial industry.

We provided a draft of this report to the FDIC in December 2015. Because our report had no recommendations, a formal response from the FDIC was not required and management opted not to provide one.