ICBA Summary of Government Accountability Office Report: *Cybersecurity – Bank and Other Depository Regulators Need Better Analytics and Depository Institutions Want More Usable Information*

August 2015

Contact:
Jeremy Dalpiaz
Assistant Vice President
Cyber Security and Data Security Policy
Jeremy.Dalpiaz@icba.org

www.icba.org

ICBA Summary of GAO Report: "Cybersecurity – Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information"

BACKGROUND

On July 2, 2015, the Government Accountability Office (GAO) published a report, "Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information"[1] ("the report"). The report focuses on an overview of responsibilities and oversight functions by banking regulators, the Federal government's effort to address critical infrastructure, the common types of cyber threats and the source of attacks.

Link to Government Accountability Office Report

OVERVIEW

This report reviews the methods that financial institutions (FIs) use to reduce vulnerabilities while also pointing out some potential shortfalls. An emphasis is put on the experience level of information technology (IT) examiners at the various agencies and where IT examiners are assigned. It also focuses on the lack of consistent data among the regulators to track data breaches and cybersecurity incidents. There is also a focus on third-party vendor examination authority.

There were two findings for areas of improvement. The first area covered data analytics. Regulators lack the ability to review deficiencies across the entire banking system. The second area covered is oversight authority. Bank regulators, on a regular basis, conduct examinations of third-party vendors. However, the NCUA (National Credit Union Administration) lacks this authority. GAO recommends that Congress give NCUA the authority to examine third-party vendors serving credit unions.

SUMMARY

FIs use various methods to reduce cyber vulnerabilities including access controls, IT security training for staff, audit functions and Interagency Guidelines. However, there are some challenges that face FIs, for instance, many may not make information security a priority until an incident occurs. There is some concern that IT staff may not be fully focused on IT as they may have other job duties, especially at smaller institutions. The report notes the comment of one vendor, to wit: "the lack of a dedicated IT security person can be a major concern for community banks, which generally are small institutions."[2] In addition the report quotes an information security vendor saying "that criminals target smaller institutions because the expected payoff is greater relative to larger institutions whose systems are generally more sophisticated and harder to compromise. Another vendor claimed that small account takeovers largely have shifted from large to medium and small institutions."[3]

Similarly, the report is not all positive for large depository institutions. Pointing out several high profile attacks against major U.S. depository institutions, the report discusses the distributed denial-of-service (DDOS) attacks in 2012 and 2013, which were conducted by a hacktivist group in the Middle East.[4] It also points out the data breach

[1] Government Accountability Office. GAO-15-509: "Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information." 2 July 2015. Available at http://www.gao.gov/products/GAO-15-509
[2] Ibid, 15.
[3] Id, 13
[4] Id, 11.

attack in 2014 against JP Morgan Chase where the "perpetrators obtained customer e-mail address, home addresses, and telephone numbers."[5] All depository institutions can experience attacks from nation-states but according to information security vendors, criminal organizations conduct the majority of cyberattacks on domestic institutions.[6] As we have learned from recent news reports, that was the case in the JPMorgan breach.[7] The report also criticizes FIs for not identifying breaches in a timely fashion.

Staffing or institution size may not be the only indicator of potential challenges; one vendor interviewed also suggested that cyberattacks will worsen as mobile banking grows.

The costs of cyberattacks are not easily quantifiable. However, the GAO tacitly references studies by the Independent Community Bankers of America (ICBA) and the Credit Union National Association (CUNA), quoting the costs of the Target and Home Depot breaches.[8] Since financial harm is not the only cost of a breach, the report acknowledges the potential of reputational risks and the fact that some FIs have purchased cyber insurance.

Bank regulators[9] "have issued guidance that addresses risk-focused examinations and incorporates best practices for information security. The guidance describes the processes examiners should follow for risk-focused supervision – in which examiners identify and then focus on the areas that pose the highest risk to institutions."[10] There is a need to ensure adequate staff with IT experience at the agencies. For instance, below is how the four banking agencies compare in terms of quantity and expertise level of IT examiners as of early 2015:

- FDIC has 60 premium IT examiners, used mostly in large institutions with highly complex IT infrastructure. There are also 32 IT examination analysts and more than 100 subject-matter experts who generally assist in reviews at small and medium size institutions.
- OCC has 100 dedicated IT specialist examiners with more than 40 assigned to review its 19 largest banks.
- The Fed has 85 IT examiners who have IT or advanced IT expertise and focus on the largest institutions.
- NCUA has 40-50 subject-matter IT examiners, 12 IT specialists in regional offices and four in headquarters. They mostly focus on the largest credit unions, but consult regularly with regular examiner staff on IT issues that arise during exams.[11]

This demonstrates that regulators "generally have not used IT experts during the examinations of medium and small institutions, which are often determined to be low risk."[12] To address improvements in information security oversight, regulators have been increasing the "numbers of staff with IT and information security expertise."[13] Referencing the newly released Cybersecurity Assessment Tool from the Federal Financial Institutions Examination Council (FFIEC), GAO acknowledges that regulators will be updating the IT Examination Handbook, along with an enhanced incident analysis process, an updated crisis management process, an expanded focus on technology service providers and enhanced collaboration with law enforcement and intelligence agencies.

[5] Id.
[6] Id, 13.
[7] See New York Times article, *"Four Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach."* http://www.nytimes.com/2015/07/22/business/dealbook/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html?_r=0. Accessed 22 July 2015.
[8] CUNA and ICBA are not mentioned specifically.
[9] These regulators include the Federal Reserve (Fed), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and the National Credit Union Administration (NCUA)
[10] GAO-15-509. 19.
[11] Id, 24-25.
[12] Ibid, 25.
[13] Id, 26.

GAO asked for information related to the "number of deficiencies identified during examinations that included information systems and technology."[14] In response, they received information that varied in detail and was not "broken into categories that differentiated the types of deficiencies found."[15] This creates difficulty for regulators to identify "broader IT issues affecting their regulated entities, and better target their IT risk assessment."[16]

Under the Bank Service Company Act, the Fed, FDIC and OCC have authority to supervise and examine third party service providers, such as technology service providers and typically coordinate these exams. Results of the report are usually sent to only those institutions contracting with the vendor if the vendor receives low ratings for its IT practices. This assists institutions in managing their relationships and alerts them to any risks that maintaining the vendor relationship may pose.

There are significant advantages for examination authority of third-party vendors by the banking regulators. For instance, the use of third-party vendors can add operation and reputational risks to an institution. Managing these vendors, or providers, "can be difficult because smaller institutions may lack leverage in their contractual relationships to obtain information to help them determine whether providers have been performing adequately."[17] In other words, this examination authority helps small institutions meet their regulatory due diligence requirements. GAO has repeatedly reported that "joint regulatory examinations of third-party service providers might increase the economy and efficiency of federal oversight of Internet banking activities."[18] Finally, the report points out that a "deficiency in a third-party providers' operations quickly could become deficiencies that produce financial and other harm…"[19] Performing these joint examination exercises helps to protect the entire banking system against these deficiencies. However, the NCUA lacks authority to examine third-party vendors[20] and GAO, ICBA, NCUA and the Financial Stability Oversight Council (FSOC), support this authority. The GAO suggests legislation to give NCUA said authority.

There is significant data flow from government sources (Department of Homeland Security, law enforcement agencies, National Cyber Investigative Joint Task Force and the Secret Service) to FIs as well as the information flow amongst public-private partnerships via the Financial Services-Information Sharing and Analysis Center (FS-ISAC). However, smaller financial institutions face a challenge in deciphering the amount of information being transmitted to them.[21] Treasury has acknowledged this is an area they will work on. Meanwhile, FS-ISAC and the Depository Trust Clearing Center have developed and deployed "Soltra Edge," to disseminate alerts to member institutions with the goal of giving potential victims a fuller picture of the threat using standardized language. To date, many large institutions have adopted the technology.[22]

CONCLUSION

Banks are prepared to guard against data and cyberattacks and are utilizing many different methods to gather and share actionable intelligence for the purpose of protecting customer data. However, the GAO Report illuminates the need for experienced IT examiners, not just at the largest banks, but also community banks. Small institutions face comparable cyber and data security threats as large institutions and should be privy to the same level of expertise during an IT examination. Examiners would do well to focus their efforts on consistent data collection among the regulators to track breaches and cybersecurity incidents. Finally, throughout the report GAO made clear the overwhelming advantages of third-party vendor examinations. All sectors of the financial industry would benefit from an examination of all vendors.

[14] Id, 27.
[15] Id.
[16] Id, 29.
[17] Id, 29-30.
[18] Id, 32.
[19] Id, 32.
[20] NCUA's authority to examine third-party vendors expired in December 2001. In lieu of this, NCUA has instituted a risk focused examination program.
[21] Id, 39.
[22] Id, 33-34.