July 2015

CYBERSECURITY

Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information

GAO Highlights

Highlights of GAO-15-509, a report to congressional requesters

Why GAO Did This Study

Depository institutions experienced cyber attacks in recent years that are estimated to have resulted in hundreds of millions of dollars in losses. Depository institution regulators (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, and NCUA) oversee information security at these institutions and Treasury coordinates protection of the financial sector.

The objectives of this report include examining (1) how regulators oversee institutions' efforts to mitigate cyber threats, and (2) sources of and efforts by agencies to share cyber threat information. GAO collected and analyzed cyber security studies from private-sector sources. GAO reviewed materials from selected IT examinations (based on regulator, institution size, and risk level). GAO also held three forums with more than 50 members of financial institution industry associations who provided opinions on cyber threat information sharing.

What GAO Recommends

Congress should consider granting NCUA authority to examine third-party technology service providers for credit unions. In addition, regulators should explore ways to better collect and analyze data on trends in IT examination findings across institutions. In written comments on a draft of this report, the four regulators stated that they would take steps responsive to this recommendation.

View GAO-15-509. For more information, contact Lawrance Evans, (202) 512-8678, or evansl@gao.gov

What GAO Found

Regulators use a risk-based examination approach to oversee the adequacy of information security at depository institutions—banks, thrifts, and credit unions—but could better target future examinations by analyzing deficiencies across institutions. For information technology (IT) examinations, regulators adjust the level of scrutiny at each institution depending on the information they review, past examination results, and any IT changes. GAO reviewed 15 IT examinations and found that regulators generally reviewed institutions' policies, interviewed staff, and examined audits of information security practices. While the largest institutions were generally examined by IT experts, medium and smaller institutions were sometimes reviewed by examiners with little or no IT training. The regulators recognized that some IT training is necessary for all examiners, so each regulator had efforts under way to increase the number of their staff with IT expertise and conduct more training. GAO identified two areas for improvement:

- **Data analytics**. Regulators generally focused on IT systems at individual institutions but most lacked readily available information on deficiencies across the banking system. Although federal internal control standards call for organizations to have relevant, reliable, and timely information on activities, regulators were not routinely collecting IT security incident reports and examination deficiencies and classifying them by category of deficiency. Having such data would better enable regulators to identify and analyze trends across institutions and use that analysis to better target areas for review at institutions.

- **Oversight authority**. Bank regulators directly address the risks posed to their regulated institutions from third-party technology service providers, but the National Credit Union Administration (NCUA) lacks this authority. Cyber risks affecting a depository institution can arise from weaknesses in the security practices of third parties that process information or provide other IT services to the institution. Bank regulators routinely conduct examinations of service providers' information security. Authorizing NCUA to routinely conduct such examinations could help it better ensure that the service providers for credit unions also follow sound information security practices.

Depository institutions obtain cyber threat information from multiple sources, including federal entities such as the Department of the Treasury (Treasury). Representatives from more than 50 financial institutions told GAO that obtaining adequate information on cyber threats from federal sources was challenging. Information viewed as most helpful for assessing threats and protecting systems included details on attacks other institutions experienced. To help address these needs, Treasury has various efforts under way to obtain such information and confidentially share it with other institutions. The department formed a special group that works with other law enforcement and intelligence agencies to obtain declassified information and share it with financial institutions in a series of circulars. Treasury staff also participate in Department of Homeland Security groups that monitor cyber incidents and work with a center that provides cyber threat information to thousands of financial institutions.