paBanker
THE OFFICIAL MAGAZINE OF THE PENNSYLVANIA BANKERS ASSOCIATION
Winter 2016 | Volume 18.6

FINANCIAL EDUCATION

PROFESSIONAL DEVELOPMENT WITH PA BANKERS

ELECTION/END OF LEGISLATIVE SESSION RECAP

FOCUS ON: BANKING IN TOMORROW'S WORLD

Bank Regulators' Concerns About Cybersecurity Has Not Abated: Greater Pressure on the Board of Directors is Expected

In July 2015, the Comptroller of the Currency Thomas J. Curry stated that cyber threats were the foremost risk facing banks. He also said that cyber threats are "one of the major, if not the major, risk facing businesses of all sorts."

President Obama recognized the unique risks posed by cyber threats by including a request for more than $19 billion in his 2017 budget and creating a new commission on enhancing cybersecurity to address cybersecurity issues within the government.

An increasing number of cyber attacks in the past several months, whether in the political arena, medical profession or in the financial services industry, have caused banking regulators to increase their diligence over a depository institution's ability to protect against cyber incursions. Even the banking regulators were not immune from cyber attacks, as it was discovered that the FDIC was subjected to several cyber incidents over the last couple years, putting the personal information of over 160,000 individuals at risk. Most recently, the OCC was subjected to a major information security incident involving the unauthorized removal of more than 10,000 records containing privacy information.

The increased diligence came on the heels of a July 2015 report by the Government Accountability Office (GAO) which was highly critical of the banking regulators' ability to properly examine depository institutions for information security. The GAO found that the regulators were deficient in their ability to properly examine banks' ability to protect against cyber risks (and as noted above, the FDIC was discovered to have similar difficulties in protecting its information from cyber incursions).

The GAO conducted the study because prior examinations by prudential regulators found that depository institutions had lost hundreds of millions of dollars in recent years and that a major U.S. bank had experienced a cyber intrusion that impacted tens of millions of customers. A primary finding was that "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."

As a result of the GAO study, the bank regulators have increased their training of examiners and in Nov. 2015, the Federal Financial Institutions Examination Council (FFIEC) amended its "IT Examination Handbook" that vastly increased the obligations of a bank's board of directors to ensure that the institution is protected against cyber attacks. These amendments will direct examiners to review almost 300 new specific items of inquiry during a bank's examination.

The examiners now will focus on ensuring that the new obligations imposed on a bank's board of directors to oversee the management of the bank's cybersecurity program are properly implemented. As the new common saying within the banking community

About the Authors:

THOMAS BROOKS is Of Counsel in the Washington, DC Office of Clark Hill PLC and has served as General Counsel to the FDIC and General Counsel to the US Senate Committee on Banking, Housing and Urban Affairs.

JOANN NEEDLEMAN is a Member in the Philadelphia office of Clark Hill, PLC, where she leads the Consumer Financial Services Regulatory and Compliance Practice Group. Joann also sits on the Consumer Financial Protection Bureau's Consumer Advisory Board.

indicates, "protection against cyber attacks has been moved from the server room to the board room."

What can a board of directors expect under this new examination regime? The primary focus of the examiner will be to review the bank's governance structure to determine that the board has exercised its oversight of IT activities, verify that it has set the tone and direction for the bank's use of technology and that IT risks are adequately identified, measured and mitigated. The examiner also will verify that the board has approved the information security program and that board members are familiar with all of the bank's IT-related activities.

How will the examiner verify that the board is effective in its IT oversight responsibilities? Among many points of inquiry, the examiner will determine whether the board has developed a robust strategy that includes an information security plan that safeguards against cybersecurity threats. New board responsibilities will include ensuring management's proper due diligence on third party service providers (a growing area of concern for the regulators) and that the board has an oversight and monitoring process that includes receiving updates on major projects, IT budgets, IT priorities and overall IT performance. A board also must have an effective approval process for critical projects and activities.

The board may delegate the design, implementation and monitoring of specific IT activities to an IT steering committee of the board. However, the board remains ultimately responsible for overseeing IT activities and documenting its actions. While the implementation of these tasks might be daunting for most community banks, that will not deter the examiner from grading the bank's board of directors on its compliance with these mandates.

In order to verify that the board is effective in its IT oversight, the examiner will specifically review and determine whether or not the board does the following, among other things:

- Reviews and approves an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to safeguard against ongoing and emerging threats, including cybersecurity threats;
- Oversees the institution's adoption of effective IT governance processes;
- Oversees management processes for approving third-party providers that include an assessment of their financial condition and IT security posture, including efforts to address cybersecurity;
- Has an oversight process that includes receiving updates on major projects, IT budgets, IT priorities and overall IT performance and has an approval process for critical projects and activities;
- Reviews the adequacy and allocation of IT resources in terms of funding and personnel;
- Approves a policy to escalate and report significant security incidents to the board, steering committee, government agencies and law enforcement, as appropriate; and
- Holds management accountable for the identification, measurement and mitigation of IT risks.

Board compliance is only one of more than a dozen objectives that the examiner must accomplish during the examination. Each objective requires the examiner to review several specific activities of the board and management. Other specific areas of examination, to identify a few, include:

- Reviewing management's responsibility relating to business continuity should a cyber breach occur;
- Determining the proper insurance coverage for cyber risk (including loss of hardware, software, litigation costs, damages from depositor suits, etc.);
- Identifying enterprise risk management;
- Obtaining and retention of a qualified work force; and
- Ensuring that an institution is able to identify, control and mitigate risks.

Notwithstanding the increased and focused direction to its examiners when reviewing a bank's cyber preparedness, the OCC, FDIC and the Federal Reserve Board recently published a proposal that would hold boards and senior management of large banks ($50 billion or more of consolidated assets) more

continued on page 36

continued from page 35

BANK REGULATORS' CONCERNS ABOUT CYBERSECURITY HAS NOT ABATED

accountable for implementing cyber risk management frameworks. This advance notice of proposed rulemaking also proposes that the nation's big banks take steps to ensure that board members have adequate expertise in cybersecurity. (See https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery for the Federal Register Notice.)

If issued in final form, the regulators also want service providers used by banks and/or those linked to the financial infrastructure, such as payments processors, to be held to the same cybersecurity requirements that are applicable to banks. Banks likely will have to ensure in their contracts, as well as through ongoing due diligence, that their service providers are maintaining proper procedures and are complying with all security mandates. While the proposal is envisioned to apply only to large banks, it is not unreasonable to think that the mandates ultimately will find their applicability to smaller banks as well.

To further emphasize the regulators' concerns about reporting cyber incidents, the Financial Crimes Enforcement Network (FinCEN) recently issued a new advisory to financial institutions on cyber events and cyber-enabled crime (https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf). It also updated its "Frequently Asked Questions" to supplement the advisory regarding the use of Suspicious Activity Reports (SARs). FinCEN noted that while suspicious transactions may not always involve a cyber event, relevant cyber-related information should still be included in SARs when available. Relevant cyber-related information and identifiers associated with suspicious transactions and cyber events should be reported, and the advisory provides a non-exhaustive list of items that should be included in a SAR.

Is it hyperbole to say that the cyber threats are the foremost risks facing banks today? No—it is the new reality, and a bank's boards of directors must be prepared to meet this new challenge.

NOTWITHSTANDING THE INCREASED AND FOCUSED DIRECTION TO ITS EXAMINERS WHEN REVIEWING A BANK'S CYBER PREPAREDNESS, THE OCC, FDIC AND THE FEDERAL RESERVE BOARD RECENTLY PUBLISHED A PROPOSAL THAT WOULD HOLD BOARDS AND SENIOR MANAGEMENT OF LARGE BANKS ($50 BILLION OR MORE OF CONSOLIDATED ASSETS) MORE ACCOUNTABLE FOR IMPLEMENTING CYBER RISK MANAGEMENT FRAMEWORKS.

paBanker
THE OFFICIAL MAGAZINE OF THE PENNSYLVANIA BANKERS ASSOCIATION
3897 North Front Street
Harrisburg, PA 17110

PRSRT STD
US POSTAGE
PAID
HARRISBURG PA
PERMIT #411