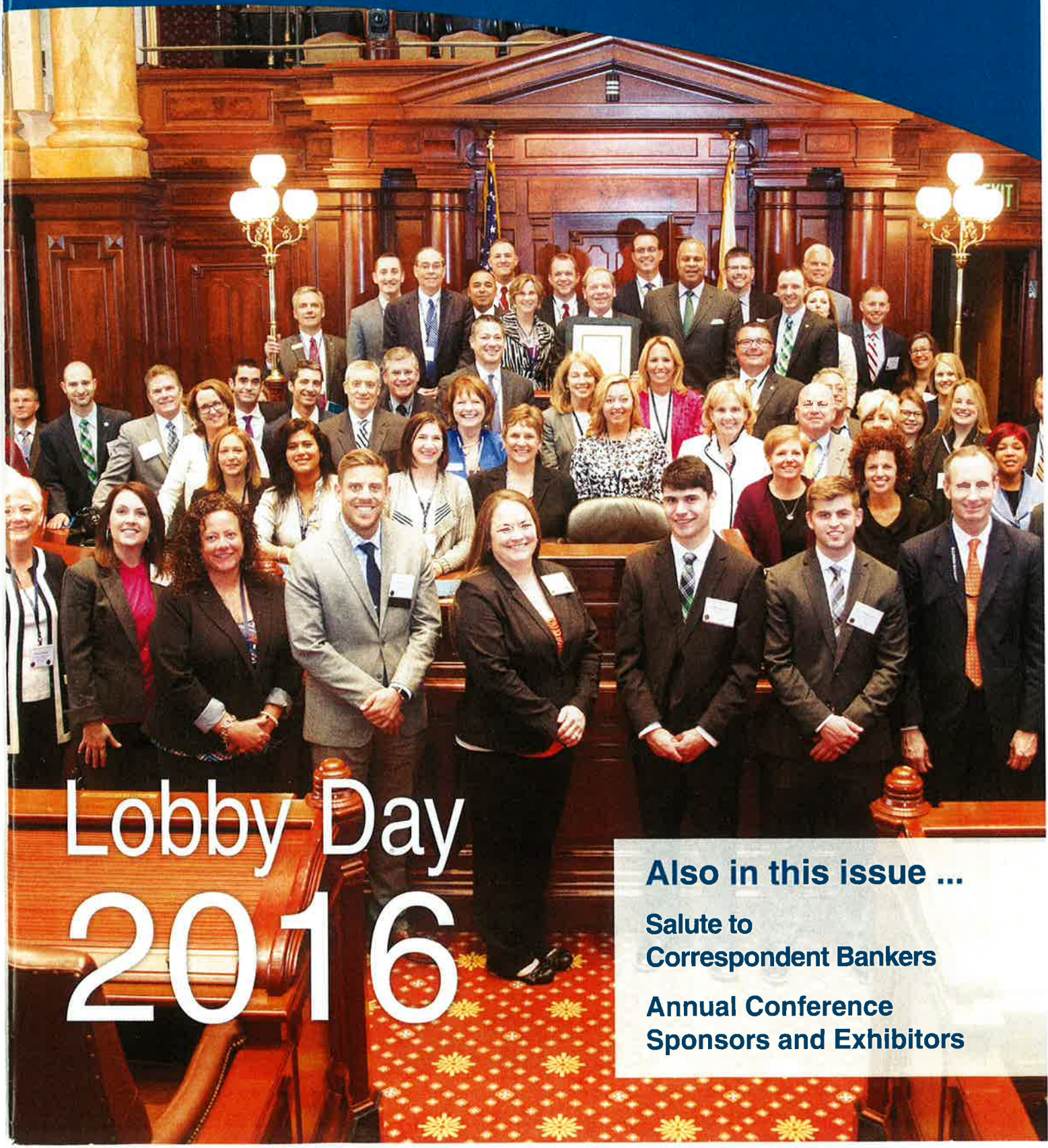
Illinois Banker

The Official Publication of the Illinois Bankers Association

May-June 2016
ilbanker.com



Lobby Day 2016

Also in this issue ...

Salute to Correspondent Bankers

Annual Conference Sponsors and Exhibitors

Cyber Threats: The Foremost Risk Facing Banks and Their Directors Today

By Thomas Brooks and John Hines Jr., Clark Hill

"Hyperbole? Not really." This is what Comptroller of the Currency Thomas J. Curry stated in a speech this past July. He also said that cyber threats are "one of the major, if not the major, risk facing businesses of all sorts." And President Obama recognized the unique risks posed by cyber threats by requesting more than $19 billion in his 2017 budget and creating a new Commission on Enhancing Cybersecurity to address cybersecurity issues in the government.

Curry's statement came on the issuance just weeks before of a report by the Government Accountability Office (GAO) 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.

The GAO conducted the study because it found that depository institutions had lost hundreds of millions of dollars in recent years as a result of cybersecurity incursions and that, in one case, a cyber-attack on a major U.S. bank had 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 November 2015, the FFIEC amended its IT Examination Handbook that will vastly increase 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.

While each regulator's guidance to its examiners might differ slightly from the provisions in the FFIEC's amended Handbook, the examiners will focus on the new obligations imposed on the board of directors to oversee the management of the bank's cybersecurity program. As the new mantra has been phrased, "protection against cyber-attacks has been moved from the server room to the board room."

Bank regulators have determined that their current highest priority in examining an institution is how to protect the bank and its depositors from cyber incursions — and that responsibility now rests firmly with the board of directors. To help banks assess their current cybersecurity risks and overall cybersecurity preparedness, the FFIEC developed the Cybersecurity Assessment Tool (CAT). While use of the CAT is voluntary, some regulators have instructed examiners to evaluate banks on how they have used this tool.

What can a board of directors expect under this new examination regime? A primary focus will be to review the bank's governance structure to determine that the board has exercised its oversight of IT activities and verify that the board has set the tone and direction for the bank's use of technology and that risks are adequately identified, measured and mitigated. The examiner also will verify that the board has approved the information security program and that the board members are familiar with the bank's IT 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 strategy that includes an information security plan to safeguard against cybersecurity threats. New board responsibilities will include ensuring that management has done proper due diligence on third-party service providers and that the board has an oversight process that includes receiving updates on major projects, IT budgets, priorities and overall 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 a steering committee of the board. The steering committee is typically responsible for strategic IT planning, oversight of performance and aligning IT with business needs. 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.

Any steering committee should have a charter that defines its responsibilities and report to the board on the status of IT activities. The reports enable the board to make decisions without having to be involved in routine activities. While the board may delegate the design, implementation and monitoring of certain IT activities to the steering committee, it remains responsible

for overseeing IT activities and providing a credible challenge to management.

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 financial condition and IT security posture of the third party, including on 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.

The above descriptions provide a brief glimpse of what the examiner will be reviewing during the examination to determine a board's compliance with its oversight of the IT activities of a financial institution. This 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 include:

- A review of 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.);
- Enterprise risk management;
- Obtaining and retention of a qualified work force; and
- Ensure that an institution is able to identify, control and mitigate risks.

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

Looking at all of this as a "glass half-full," CAT may come as a measure of good news to some banks. Like many organizations in other industry sectors, many banks have been struggling to get their arms around the concept of cyber security and, specifically, how to map technical, administrative and physical safeguards to the evolving threat of cyber intrusion. Often these struggles are internal. Bank stakeholders may differ in how they prioritize security in the context of other organizational agendas or in how they articulate and prioritize the components of a security program. CAT offers the prospect of beginning to add some clarity to the governance processes and the decision-tree as it relates to cyber security. **B**

About the authors: Thomas Brooks, Clark Hill, is the former General Counsel of the U.S. Senate Committee on Banking, Housing and Urban Affairs and Counsel of the Senate Subcommittee on Housing. He concentrates his practice in financial services and represents clients before state and federal financial institution regulatory agencies as well as before Congress and the Executive Branch of government. John Hines Jr., is a member of Clark Hill's Intellectual Property Practice Group. He concentrates in intellectual property, technology licensing, cloud computing, technology procurement, outsourcing, electronic commerce and information management. Clark Hill is an IBA Associate Member.