

ABA BANKING JOURNAL

NOV | DEC
2015

aba.com/BankingJournal



doing the
**RIGHT
THING**

DAN BLANTON

2015-2016

ABA CHAIRMAN

ALSO PREDICTIVE ANALYTICS > STRESS TESTING > M&A COMMUNICATIONS > INTERVIEW WITH TOM CURRY

CYBERSECURITY SELF-ASSESSMENT TOOL



Helps Combat Risk

A new assessment tool issued in June by federal regulators helps financial institutions identify risks and measure cybersecurity.

BY DEBRA COPE

The real and growing threat of cyberattacks against financial institutions has firmly established cybersecurity as a C-suite and boardroom priority. With the introduction of the federal financial regulatory agencies' Cybersecurity Assessment Tool, banks are gaining a new resource to help them measure, demonstrate and continuously monitor their preparedness. But they also face new implementation challenges.

Unveiled in June by the Federal Financial Institutions Examination Council, the assessment tool was designed to help institutions identify their inherent risks and determine their cybersecurity maturity across five risk areas. Its issuance culminated more than a year of intensive work by the FFIEC's Cybersecurity and Critical Infrastructure Working Group, and underscores the importance of calibrating a bank's cybersecurity posture to its individual activities and risks.

The working group laid a foundation in 2014 by conducting a four-week pilot program evaluating 500 community institutions' capacity to mitigate cyber risks. The findings shaped the development of the assessment tool, which aligns with the FFIEC Information Technology Examination Handbook and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

"It's not a silver bullet or a stand-alone," says Bethany Dugan, deputy comptroller for operational risk at the OCC. "It is one more resource for bankers to help understand their potential risk exposure and profile and to gauge where they stand in being able to deal with the threats."

Importantly, Dugan says, "it provides a common point of view on cybersecurity. We heard from institutions and bankers that we supervise that that was one of things they were looking for."

Use of the tool by banks is optional—with an asterisk. In separate letters to the institutions they supervise, the FDIC says its examiners will discuss the tool with management during exams to make sure they are aware of it; the OCC states that its examiners will gradually incorporate the assessment into bank exams; and the Federal Reserve Board notes that it would begin to use the assessment tool in the exam process by early 2016.

In other words, "It's voluntary until the examiners come in and say, 'Why didn't you do this?' Then suddenly it's not so voluntary anymore," says Kevin Petrasic, a partner in the Washington, D.C., office of the law firm Case and White LLP.

Two key components

The assessment has two parts. First, management evaluates



the institution's inherent risk, which encompasses the type, volume and complexity of the institution's operations, plus threats directed at the institution.

"It is important to be able to say, 'What is the landscape of what I look like in technology, connections and delivery channels? How is my organization put together? What are the risks that can come to me?'" Dugan says. "Then you have to turn to 'How well am I prepared? How good is my governance over those risks that I have? How strong is my control structure?'" she adds.

That's where the second part of the assessment begins. Once management understands the institution's inherent risk, it can gauge cybersecurity maturity according to five risk areas, which the assessment calls "domains." These domains are cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience. The ratings in each area are, in ascending order, baseline, evolving, intermediate, advanced and innovative.

A major objective of this process is "bringing IT to the board," says Anthony Scarola, EVP and director of technical information security at TowneBank, a \$6.1 billion bank based in Suffolk, Va. This means demonstrating "where the bank lies on the inherent risk trajectory and translating that to the financial experts sitting in board and executive-level positions who do not have the background to perform that kind of analysis." By providing a common framework and vocabulary for talking about cybersecurity, the assessment "is one tool for the industry that is a value-add," he says.

"The main message to board members is to engage management in discussions on cyber-preparedness to understand the institution's vision, risk appetite and overall strategic direction. Additionally, the board should review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threat," the Fed notes in a statement to the *ABA Banking Journal*.

Industry interest in the assessment tool has been strong. The OCC, for instance, had a webinar that drew more than 1,000 participants. "It was very interactive, with a 35- to 40-minute presentation plus a question-and-answer session for the remainder of an hour and a half," Dugan says. Bankers asked the OCC to explain the define terms and wanted to know how examiners would use the tool.

The Fed says the tool will be updated "as threats, vulnerabilities and operational environments evolve," but cautioned that banks must monitor their own operating environment and act swiftly to mitigate threats.

COMMERCE DEPARTMENT: Cybersecurity a Major Priority for U.S., World Economy

Cybersecurity is just one of many issues Bruce H. Andrews juggles in his role as U.S. Deputy Secretary of Commerce. The department, after all, has a large portfolio that is as varied as promoting international trade, overseeing the National Weather Service and keeping the U.S. Patent and Trademark Office humming.

But cybersecurity has a special pull on Andrews, the department's standard bearer on the issue. And that is not simply because his purview as the No. 2 official at the Commerce Department includes the National Institute of Standards and Technology, the author and keeper of the NIST Cybersecurity Framework.

Andrews cut his teeth on cybersecurity in the spring of 2009 upon joining the Senate Commerce Committee as general counsel. Then-Chairman Jay Rockefeller (D-W.Va.) put him straight to work on the first draft of comprehensive cybersecurity legislation. Though the bill was debated extensively, it became a political football and was not enacted; Rockefeller did, however, have some influence on President Obama's decision to issue the 2013 executive order that yielded the NIST framework. "I worked intensively on the issue for two and a half years," Andrews says. "And how the debate has changed over the course of time!"

A key difference is that only six years ago, "most people in the private sector, including large technology companies, said 'we've got cybersecurity under control,'" Andrews recounts. Today—a generation later in the warp-speed reality of technological innovation—there is deeper understanding of how critical the risks are and how interlinked entities are. Andrews noted that the number of devices connected to the Internet is expected to triple to 50 billion in the next five years.

"Cybersecurity is a major priority for the Department of Commerce because of the potential economic impact from the breaches we already see taking place, and also because of potential damage from increased cybersecurity threats," Andrews says.

It is also an area where American innovation has created opportunities. He exudes enthusiasm as he recounts how he recently led a trade mission to Romania and Poland for 20 U.S. cybersecurity companies and held a cybersecurity summit with 11 adjoining countries. Closer to home, he has convened numerous small group and outreach meetings to drive adoption of the NIST framework.

Andrews gives the banking industry solid marks for how it is grappling with threats that include denial-of-service attacks, theft of intellectual property and network and system intrusions.

"There is strong recognition in the banking sector of how important and also how existential cyber threats are." In corporate America broadly, however, "it is a very mixed bag. There are some that frankly have not been taking it as seriously."

Time and resources

A key question is how much time banks will need to perform assessments. The regulatory agencies estimated it will take an average of 80 hours—but the key word is “average.”

“Every bank is different. Everybody understands that,” says Scarola. At some smaller institutions, he notes, the head of cybersecurity wears multiple hats in IT leadership and risk management. “If they’ve got all the answers because they manage the IT side, it clearly will take less time,” Scarola says. It’s possible for such an institution to complete an assessment in one or two weeks.


But as an institution’s size and complexity increases, the security expert within IT, like Scarola himself, has to budget time for coordinating with others within IT and across the organization. “With close to 1,500 employees, more time is required. You’ve got to work with other people’s schedules,” says Scarola, who is co-chair of ABA’s Cyber and Information Security Working Group and a member of the Community Institution Advisory Board of the Financial Services Information Sharing and Analysis Center.

Some of the tasks involved in setting up the tool are mundane but necessary. The FFIEC delivered

the assessment in PDF format. “You basically need to copy-paste it to put it into your files and databases to automate the risk calculations,” Scarola says.

For TowneBank, he found it workable to put into a Microsoft Access database, where he could create ports for internal clients to access various parts of the tool.

The fact that the assessment tool is an outgrowth of a pilot test for community banks underscores its value to community banks, but also its potential challenges. “My perception is that the assessment tool is as much—if not more—directed at the smaller institutions versus larger ones,” Petrasic says. “Smaller institutions have been forewarned that they are particularly vulnerable to hackers.”

The key takeaways for C-level executives and board members are really pretty simple, Petrasic adds. Read the guidance. Talk with whomever is charged with managing the institution’s cybersecurity. Understand and make clear how critical this issue could be for an institution that doesn’t get it right. “These are not speculative issues anymore. These are real and important issues for the board and management to ponder and discuss,” he says. 

.....
DEBRA COPE is a financial writer in Washington, D.C.

Providing real-world Solutions for Financial Institutions



WATKINS CONSULTING

Cybersecurity ♦ Risk Management ♦ Compliance ♦ Litigation Support

Watkins Consulting has been providing solutions to the Financial Community for over two decades. Through every financial cycle, Watkins Consulting has provided solutions for Compliance, Litigation, and Risk Management. As Financial Institutions are increasingly facing the growing crisis of Cyber Crimes, Watkins Consulting is positioned to provide real, actionable solutions.

Watkins Consulting integrates decades of Compliance Monitoring and Risk Management experience with the technical expertise of strategic partners to help our clients proactively combat Cyber Crime. Watkins Consulting will evaluate your NIST or FFIEC Cyber Readiness and regulatory compliance. Our risk management tool, Cyber Rx, provides a straightforward method to create or improve your cybersecurity governance to mitigate Cyber Risk threats. Beyond risk management, Watkins Consulting, along with our strategic partners, can mobilize specialists in intrusion detection, breach prevention, and disaster recovery.

For more information contact us at solutions@watkinsconsulting.com or (888) 320-2320.

www.watkinsconsulting.com
 888 Bestgate Road, Suite 401, Annapolis MD 21401