WEB SEMINAR
SPONSORED BY
Appway
HOSTED BY
AMERICAN BANKER
REGISTER TODAY

AMERICAN BANKER

Cybersecurity to Gain New Prominence in Bank Exams

By Ian McKendry
November 12, 2015

WASHINGTON — Bank regulators are planning to make cybersecurity a higher priority during bank exams as early as the second quarter of next year.

While cybersecurity has already been part of bank exams for years, the Federal Deposit Insurance Corp. is planning to rework its community bank program to break cybersecurity out as its own separate issue in examination comments.

"The new program includes enhancements to specifically address cybersecurity elements," said Mark Moylan, deputy director at the FDIC's office of risk management supervision, during a community bank advisory meeting last week. "The focus on cybersecurity needs to move from the server room to the board room."

Dana Syracuse, a managing director at K2 Intelligence and former associate general counsel at the New York State Department of Financial Services, said including cybersecurity as its own comment in an exam "draws attention to it."

"The tone at the top is crucial," Syracuse said. This action will force bank executives to recognize that cybersecurity is "crucial for a regulator."

Count on us for a wide range of correspondent banking solutions.
Learn more
BMO Harris Bank
We're here to help.
BMO Harris Bank N.A. Member FDIC

Regulators want to ensure that there is an understanding of "cyber risk as it overlays into business decisions that you make at the board level," Moylan said.

He added that something like outdated systems has typically been viewed as a budget capital improvement decision, but the threat environment has changed.

"Does that change your thought process at that level as you now consider the vulnerabilities that you may have exposed your institution to because the threat environment has changed?" he asked.

Moylan also warned that if an institution has a cyber-breach "it will not be a capital event; it will be an operational event" and compared to a liquidity problem.

"You have customers that you will not be able to meet their needs, they become panicked and in respective of your capital, your asset quality, your focus will be on how quickly you are able to respond and have the right assets," Moylan said. "This is a 0-100, first hour, second hour type of scenario."

The move follows the release of a cybersecurity assessment tool that was published by the Federal Financial Institutions Examination Council earlier this year. The tool maps to the National Institute of Standards and Technology's cybersecurity framework and helps guide banks as they assess their cybersecurity defenses. It is voluntary, but examiners will be using it in the field when assessing banks.

"Use of the tool is optional, but in reality the bankers are saying that when the examiners come into their institutions that they are asking to see whether they have completed the self-assessment and asking to look at its contents," said Pamela Perdue, executive vice president of regulatory operations at Continuity, a compliance management solutions provider for community banks.

Moylan said "certainly [examiners] will look at and want to look at the tool if it is also part of your information security program and assessment."

Kevin Petrasic, a partner at the law firm White & Case, also said "If something goes wrong I don't think any CEO or senior management group really wants to be the one to say, 'Well, it's voluntary.'… At that point you are not only going to have to deal with the regulators, you are going to have to deal with other actions."

Other changes to the bank exam process will include a questionnaire that a bank will get roughly three months before an exam. An institution will have two weeks to fill out the seven-page form, which will replace a phone call or interview that has been done in the past. The FDIC will also be dropping the 15-page IT officers' questionnaire.

Moylan said the new questionnaire should be "less burdensome" and give banks more time to prepare and relay information to examiners.

"It will allow examination staff to more effectively risk scope an examination, to better customize forthcoming informational requests and insure that the suitable examination staff is assigned commensurate with the complexity of the institutions information technologies," he said.

Another change, Moylan said, is that the FDIC is likely to provide exam component ratings instead

of just the composite ratings. This "should lead to enhanced discussions with the bank board of directors and management on specific areas of strengths and weaknesses within the IT function," he said.

The FDIC is also working on similar changes to exams for third party service providers and creating an assessment tool for them. Moylan said that he wants banks to review their contracts with third party service providers and make sure the contracts and performance meet their expectations.

"What I don't want a community bank to say is, I don't have to worry about [cybersecurity] because I am serviced."

The FDIC is in the process of finalizing the new exam program and once approved, a pilot test program will be used in selected offices in the first quarter of 2016 with implementation planned for mid-2016.

© 2015 SourceMedia. All rights reserved.
Mobile Version