Bloomberg GOVERNMENT

»BGOV Analysis
Aug. 6, 2014

Finance in the Cyber Crosshairs

As regulatory scrutiny of cybersecurity preparedness intensifies, more requirements may be on the way

BY SANFORD REBACK
Bloomberg Government Senior Technology Analyst

TONY COSTELLO
Director of Government Affairs Research

RELATED ANALYSIS

Cyberattacks Rise: Mandatory Standards Coming?

EU Raises Specter of Tough Internet Regs

'Big Data' Reports May Lead to Big Privacy Change

FINDINGS

Despite the Obama administration's professed preference for voluntary standards rather than mandatory requirements to enhance cybersecurity in the private sector, more cybersecurity requirements may be on the way for financial services companies.

» Several agencies, at both federal and state levels, have instituted enhanced oversight of financial services companies' cybersecurity readiness in the last few months. Enforcement actions and fines could follow.

» This new regulatory attention will result in increased costs for businesses, as companies revise internal procedures and boost their spending on cyberdefenses.

» It's possible that the Securities and Exchange Commission (SEC) may institute more specific requirements that would require all public companies — not just financial services firms — to disclose more about the cyberattacks they suffer. Regulators could also establish a cybersecurity preparedness certification requirement, analogous to that mandated by the Sarbanes-Oxley legislation, and make some adjustments to existing regulations.

WHAT'S AHEAD

It's not clear whether some financial services companies' call for greater government/private-sector cooperation to boost cybersecurity will be sufficient to stave off the imposition of new regulatory requirements. Bloomberg News has reported that the Securities Industry and Financial Markets Association (SIFMA) recently proposed the establishment of a government-industry cyber war council to protect against cyberattacks.

Prospects for legislation intended to boost information sharing between the government and the private sector about cyberattacks are also uncertain. The full Senate probably won't consider a bill approved by the Senate Intelligence Committee before the November midterm elections. Differences with a House bill would also need to be resolved.

Recent Cybersecurity Actions by Financial Services Regulators

Regulator	Action
Securities and Exchange Commission	Cybersecurity examinations of more than 50 broker-dealers
Federal Financial Institutions Examination Council	Cybersecurity assessments of 500 community banks
State of New York	New targeted assessments of the banks it regulates
Financial Industry Regulatory Authority	Letters sent to 20 broker-dealers asking about their cybersecurity practices

Sources: Regulatory agencies listed above

BACKGROUND

The security of the financial services sector has long been vital to the U.S. Viewed broadly, the sector provides credit and liquidity to customers, allows them to invest funds and make payments, and enables them to transfer risk. The sector was designated one of 16 critical infrastructure sectors by a presidential policy directive in 2013.

In the wake of recent high-profile cyberattacks at U.S. retailers such as Target Corp. and reported incursions at a number of U.S. financial services companies, U.S. officials have increased their calls for better cybersecurity at financial institutions. Most recently, Treasury Secretary Jacob J. Lew decried the status of U.S. cybersecurity defenses as insufficient and said companies "should and could be doing more" to improve them.[1] During his July 16 speech at the Delivering Alpha conference in New York, Lew also announced that Deputy Treasury Secretary Sarah Bloom Raskin would be working with federal and state regulatory bodies to reduce cyber-risks, saying that she would be "looking beyond traditional financial services to explore the regulatory, security and consumer protection aspects of financial technology."

Lew's comments were the most recent and prominent of a number of remarks by government officials expressing concern over the status of the financial sector's cyber preparedness. The SEC held a roundtable in Washington on March 26 at which the status of cybersecurity defenses in the financial markets and among broker-dealers, investment advisors and transfer agents was a prominent part of the discussion.[2] SEC Commissioner Luis Aguilar warned corporate boards about the dangers of ignoring cyber-risk during a June 10 speech at a conference sponsored by the New York Stock Exchange.[3]

REGULATORY SCRUTINY

Several government agencies with supervisory authority over segments of the financial services industry have announced new regulatory oversight programs in the last several months. The following is a discussion of a few prominent examples.

Securities and Exchange Commission

The SEC's Office of Compliance Inspections and Examinations (OCIE) announced April 15 that it would conduct examinations of more than 50 registered broker-dealers and investment advisors to assess their cybersecurity preparedness.[4] Along with the announcement, OCIE included an illustrative list of questions it may use as it conducts examinations.

Among the areas OCIE plans to investigate, based upon the questionnaire, are the target company's:

- Cybersecurity governance structure.
- Identification and assessment of cybersecurity risks.
- Protection of its networks and information.
- Risks associated with vendors and other third parties.
- Methods of detecting unauthorized activity on its networks.
- Experiences with certain cybersecurity risks.

The examinations could result in enforcement actions against companies whose cybersecurity systems or defenses are deemed insufficient.

Separately, the SEC has reportedly opened investigations of multiple companies in recent months, examining whether they properly handled and disclosed cyberattacks.[5] These investigations aren't limited to, and may not involve, financial services companies.

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) announced on May 7 a pilot cybersecurity assessment designed to enable federal and state banking regulators to "assess the vulnerability of community institutions to cyber threats and their preparedness to mitigate cyber-risks."[6] Bank examiners have been assessing the cyber preparedness of 500 community banks.

The FFIEC is an interagency government body with the power to set uniform principles, standards and reporting forms for the examination of financial institutions by the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau. A liaison body representing state banking supervisors also is a voting member of the council.

The cybersecurity assessments, which will be undertaken as part of the regular examinations scheduled for financial institutions, will focus on the following aspects of cybersecurity preparedness:

- Risk management and oversight.
- Threat intelligence and collaboration.
- Cybersecurity controls.
- External dependency management.
- Cyber-incident management and resilience.

The financial regulators conducting the examinations will have the ability to take enforcement actions and "communicate necessary corrective action" if cybersecurity measures in place are deemed insufficient.

State of New York

New York Governor Andrew Cuomo announced May 6 that the state Department of Financial Services (DFS) will conduct "new, regular, targeted cyber security preparedness assessments" of the banks it regulates.[7] Cuomo said the primary purpose of the assessments is to help protect New Yorkers' finances from online predators and secure personal bank records from being breached.

The assessments will be conducted as part of the regular DFS examination process and will be designed to drive a consistent focus on cybersecurity preparedness. The examination procedures will include additional questions in the areas of IT management and governance, incident response and event management, access controls, network security, vendor management and disaster recovery.

DFS will release more details about the timing and content of the examination procedures in coming weeks.

Financial Industry Regulatory Authority

The Financial Industry Regulatory Authority (FINRA) announced in February that it had sent about 20 broker-dealers letters asking about how they manage cybersecurity threats.[8] FINRA, the nonprofit regulator of the securities industry, said it sent the letters to better understand how companies manage these threats and to increase its understanding of company vulnerabilities.

Among other things, the letters sought information on company approaches to information technology risk assessment, business continuity plans in the event of a cyberattack, how companies handle distributed denial-of-service attacks, and the effect that cyberattacks have had on companies in the last year.

While the primary focus of the FINRA letters appears to help it gain a better understanding of the scope of cyberthreats that securities companies face, information gleaned through the process could also be used for follow-up investigations or enforcement actions.

NEXT REGULATORY STEPS?

Stepped-up enforcement actions, or even the threat of such actions, may provide financial services regulatory authorities sufficient leeway to boost company cybersecurity preparedness. Even so, more onerous regulatory requirements also could be in the offing. This section discusses three prominent suggestions.

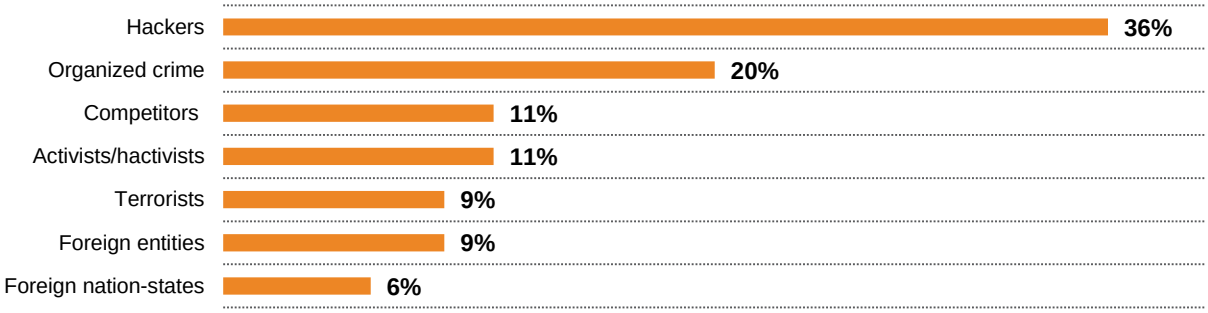
Increased Disclosure

The SEC in 2011 issued guidance clarifying that public companies are required to publicly disclose cybersecurity threats and attacks that are material to their businesses. Since then, questions have been raised regarding whether the disclosure requirements need to be more explicit and extensive. Enhanced disclosure requirements would apply to all public companies, not just those in the financial services sector.

Several government officials have publicly advocated more extensive disclosure requirements in the last several weeks. Shelley Parratt, the deputy director of the SEC's Division of Corporation Finance, said May 1 that the division had found much of the disclosure relating to cybersecurity in company securities filings insufficient.[9] Speaking at a conference at Northwestern University,

Sources of Outside Cyberattacks on Financial Services Companies

Financial services firms suffer cyberattacks from hackers far more often than from nation-states.



Source: PwC, CIO Magazine and CSO Magazine, The Global State of Information Security Survey 2014

Paratt said that companies needed to consider, among other things, how information they had previously submitted to the SEC might need to be updated in light of new developments.

More recently, in his June 10 speech at a New York Stock Exchange conference, SEC Commissioner Aguilar urged companies to look beyond the requirements of securities laws when deciding whether to disclose a data breach. Whether disclosure requirements should be modified and strengthened also was a prominent topic of discussion at the SEC's March 26 cybersecurity roundtable.

It's not clear whether the SEC will mandate more extensive cybersecurity disclosure requirements in the near to mid term. Extensive disclosure of cyberattacks could highlight company vulnerabilities, for example. Whether a cyber-intrusion has had a material impact on a company may not become clear until months or even years after an intrusion has been discovered.

Rather than more-extensive disclosure, a more likely requirement would be reviewing and updating previous disclosures about cyberattacks a company had suffered. It's possible the SEC may issue guidance to that effect in the coming months. The commission could also choose to amend Regulation S-P, which deals with measures broker-dealers and other organizations must take to secure customer records and information.

Making the Framework Mandatory

Even before the National Institute of Standards and Technology (NIST) published its voluntary cybersecurity framework earlier this year, speculation abounded that the Obama administration intended to make the requirements in the framework mandatory. NIST released the framework, which is intended to help companies improve their cybersecurity practices, in February.

Administration officials have said they don't plan to make the framework mandatory. Even so, the document is well on its way to becoming a de facto standard, especially in the financial services sector. The SEC's Office of Compliance Inspections and Examinations said that some of the questions it plans to use in cybersecurity preparedness examinations of broker-dealers and investment advisers track information provided in the NIST framework. Treasury Secretary Lew and SEC Commissioner Aguilar have urged financial services companies to use the framework, and Lew has encouraged financial services companies to have their outside vendors follow the framework.

Because the framework is more a menu of options than a set of prescribed requirements, exhortations from government officials to use it won't result in a specific set of requirements that companies will have to adopt, even in the financial services sector. But companies that fail to incorporate the processes and methodology found in the framework into their internal cybersecurity practices can expect intense and skeptical questioning when financial regulators conduct their oversight examinations.

Sarbanes/Oxley-Like Certification

It's possible that the SEC could institute a requirement that senior corporate executives certify their company's cybersecurity efforts as part of the company's mandatory securities filings.

Such a requirement would be analogous to certification requirements contained in the Sarbanes-Oxley Act of 2002, which among other things requires company chief executive officers and chief financial officers to certify that the company's filed financial statements fairly present its financial condition. The law specifies fines and possible imprisonment for executives who knowingly certify inaccurate financial statements.

A cybersecurity-preparedness certification requirement could accomplish an articulated goal of senior financial services regulatory officials — increasing senior-level company focus on cybersecurity — while not necessarily prescribing exactly what steps companies must take to improve their cybersecurity preparedness, which the private sector has long resisted.

It's not clear whether legislation would be needed to establish a cybersecurity-preparedness certification requirement, or whether the SEC could essentially institute such a requirement by issuing guidance on how it would interpret current regulations.

WHAT TO WATCH

Whether the increased regulatory scrutiny of the cybersecurity preparedness of financial services companies results in enforcement actions against individual companies should be monitored closely. Even a few enforcement actions would demonstrate the increased willingness of regulatory authorities to hold financial services companies to a higher standard in terms of the policies, procedures and practices they have in place.

SIFMA reportedly recently proposed the establishment of a government-industry cyber war council to protect against cyberattacks in the financial services sector.[10] The proposal calls for a committee of company executives and senior representatives from the Treasury Department, the National Security Agency, and the White House, among others. It's not clear whether the proposal for greater government/private-sector cooperation to boost cybersecurity defenses will be sufficient to stave off more stringent regulatory oversight or the imposition of new regulatory requirements.

Prospects for legislation intended to boost information sharing between the government and the private sector about cyberattacks are also uncertain. The full Senate probably won't consider a bill, S. 2588, approved by the Senate Intelligence Committee before the November midterm elections. Differences with a House bill, H.R. 624, also would need to be resolved, and the entire topic may be deferred until Congress addresses NSA surveillance issues.

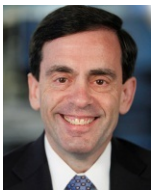
ABOUT BLOOMBERG GOVERNMENT

Bloomberg Government is the only comprehensive web-based information service for professionals who are affected by and interact with the federal government. Bloomberg Government provides rich data, analytical tools, timely news and in-depth analysis from policy experts — all from the leader in business information services.

ANALYST CONTACT INFORMATION

Sanford Reback, Senior Technology Analyst sreback1@bloomberg.net +1 202 416 3421

ABOUT THE ANALYST



Sanford Reback is a Senior Technology Analyst with Bloomberg Government. He previously served as an executive at MCI, then a Fortune 100 company; UUNET, then the world's largest Internet services provider; and two venture-backed technology companies. At the Office of the U.S. Trade Representative, he helped negotiate NAFTA and the World Trade Organization agreements and technology sector agreements. Reback holds a B.A. in political science from Stanford University, a J.D. from Harvard Law School, and a master's degree from Harvard's Kennedy School. He was a Fulbright Fellow in London. Follow Sandy on Twitter: @SandyReback

ENDNOTES

[1] U.S. Department of the Treasury, "Remarks of Secretary Jacob. J. Lew at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor," July 16, 2014, http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx (retrieved July 29, 2014).

[2] U.S. Securities and Exchange Commission, Transcript of Cybersecurity Roundtable, March 26, 2014, http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt (retrieved July 23, 2014).

[3] Luis A. Aguilar, "Boards of Directors, Corporate Governance and Cyber-Risks; Sharpening the Focus," speech at New York Stock Exchange Conference, June 10, 2014, http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U9qgHPldXTA, (retrieved July 30, 2014).

[4] U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, "OCIE Cybersecurity Initiative," April 15, 2014 http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf, (retrieved July 30, 2014).

[5] Dave Michaels, "Hacked Companies Face SEC Scrutiny Over Disclosure," Bloomberg News, July 2, 2014, http://www.bloomberg.com/news/2014-07-02/hacked-companies-face-sec-scrutiny-over-disclosure.html, (retrieved July 30, 2014).

[6] Federal Financial Institutions Examination Council, "Introduction to Federal Financial Institutions Examination Council's Cybersecurity Assessment," May 7, 2014, http://www.ffiec.gov/pdf/cybersecurity/2014_June_FFIEC-Cybersecurity-Assessment-Overview.pdf, (retrieved July 30, 2014).

[7] State of New York, "Governor Cuomo Announces New Cyber Security Assessments for Banks," May 6, 2014, https://www.governor.ny.gov/press/5614-cyber-security, (retrieved July 30, 2014).

[8] Yin Wilczek, "FINRA Sends Sweep Letters Asking Firms About Approach to Cybersecurity Threats," Bloomberg BNA, Feb. 11, 2014, http://www.bna.com/finra-sends-sweep-letters-asking-firms-about-approach-to-cybersecurity-threats/.

[9] Michael Bologna, "SEC Official Points to Deficiencies in Companies' Cybersecurity Disclosures," Bureau of National Affairs, May 2, 2014.

[10] Carter Dougherty, "Banks Dreading Computer Hacks Call for Cyber War Council," Bloomberg News, July 8, 2014, http://www.bloomberg.com/news/2014-07-08/banks-dreading-computer-hacks-call-for-cyber-war-council.html, (retrieved July 30, 2014).