Fresh Worries for Boards of Directors

New cyber security regulations increase exposure for directors and officers at financial institutions.

By Alex Wright

New cyber security rules for New York financial institutions went into effect in March.

Boards of directors could face a fresh wave of directors and officers (D&O) claims following the introduction of tough new cybersecurity rules for financial institutions by The New York State Department of Financial Services (DFS).

Prompted by recent high profile cyber attacks on JPMorgan Chase, Sony, Target, and others, the state regulations are the first of their kind and went into effect on March 1.

The new rules require banks, insurers and other financial institutions to establish an enterprise-wide cybersecurity program and adopt a written policy that must be reviewed by the board and approved by a senior officer annually.

The regulation also requires the more than 3,000 financial services firms operating in the state to appoint a chief information security officer to oversee the program, to report possible breaches within 72 hours, and to ensure that third-party vendors meet the new standards.

Companies will have until September 1 to comply with most of the new requirements, and beginning February 15, 2018, they will have to submit an annual certification of compliance.

The responsibility for cybersecurity will now fall squarely on the board and senior management actively overseeing the entity's overall program. Some experts fear that the D&O insurance market is far from prepared to absorb this risk.

"The new rules could raise compliance risks for financial institutions and, in turn, premiums and loss potential for D&O insurance underwriters," warned Fitch Ratings in a statement. "If management and directors of financial institutions that experience future cyber incidents are subsequently found to be noncompliant with the New York regulations, then they will be more exposed to litigation that would be covered under professional liability policies."

D&O CHALLENGE

Judy Selby, managing director in BDO Consulting's technology advisory services practice, said that while many directors and officers rely on a CISO to deal with cybersecurity, under the new rules the buck stops with the board.

"The common refrain I hear from directors and officers is 'we have a great IT guy or CIO,' and while it's important to have them in place, as the board, they are ultimately responsible for cybersecurity oversight," she said.

William Kelly, senior vice president, underwriting at Argo Pro, said that unknown cyber threats, untested policy language and developing case laws would all make it more difficult for the D&O market to respond accurately to any such new claims.

Insurers, on their part, will need to account for the increased exposures presented by these new regulations and charge appropriately for such added exposure."

—William Kelly, *senior vice president, underwriting, Argo Pro.*

"Insurers will need to account for the increased exposures presented by these new regulations and charge appropriately for such added exposure," he said.

Going forward, said Larry Hamilton, partner at Mayer Brown, D&O underwriters also need to scrutinize a company's compliance with the regulations.

"To the extent that this risk was not adequately taken into account in the first place in the underwriting of in-force D&O policies, there could be unanticipated additional exposure for the D&O insurers," he said.

Michelle Lopilato, Hub International's director of cyber and technology solutions, added that some carriers may offer more coverage, while others may pull back.

"How the markets react will evolve as we see how involved the department becomes in investigating and fining financial institutions for noncompliance and its result on the balance sheet and dividends," she said.

Christopher Keegan, senior managing director at Beecher Carlson, said that by setting a benchmark, the new rules would make it easier for claimants to make a case that the company had been negligent.

SUMMARY

- ***New cybersecurity rules*** place added burdens of financial institutions.
- ***Boards of directors*** will bear the brunt of compliance responsibility.
- ***Companies must establish*** cybersecurity programs and vet vendors.

ASPEN
INSURANCE

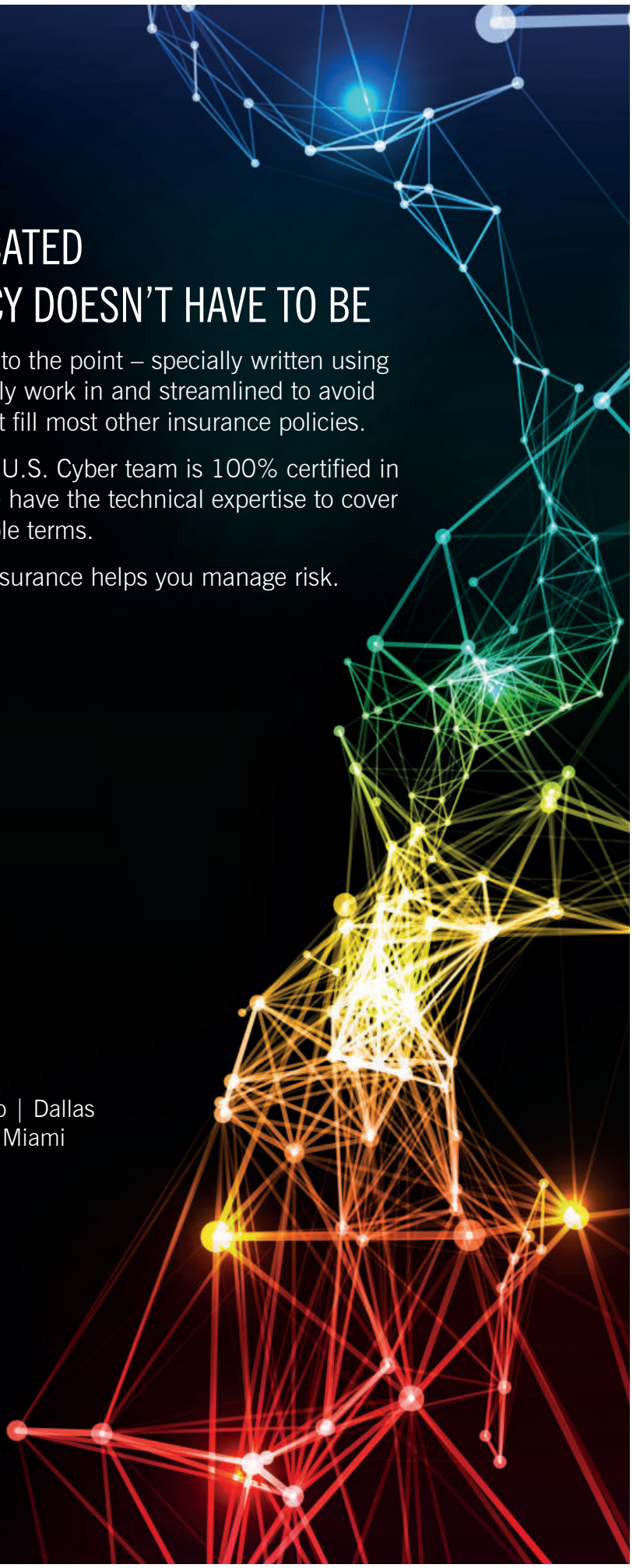
CYBER RISK IS COMPLICATED YOUR INSURANCE POLICY DOESN'T HAVE TO BE

The Aspen APEX policy is clear and to the point – specially written using the network terminology you naturally work in and streamlined to avoid the extra clauses and exclusions that fill most other insurance policies.

Unlike some insurance carriers, our U.S. Cyber team is 100% certified in Privacy and/or Network Security. We have the technical expertise to cover your exposure and explain it in simple terms.

It's just one more way that Aspen Insurance helps you manage risk.

Find out more at
aspen-insurance.com



OUR U.S. OFFICE LOCATIONS

Atlanta | Baltimore | Boston | Chicago | Dallas
Houston | Jersey City | Los Angeles | Miami
New York | Philadelphia | Rocky Hill
San Francisco | San Juan, PR

"If stock prices drop, then this makes it easier for class action lawyers to make their cases in D&O situations," he said. "As a result, D&O carriers may see an uptick in cases against their insureds and an easier path for plaintiffs to show that the company did not meet its duty of care."

One area that regulators and plaintiffs might seize upon is the certification compliance requirement, according to Rob Yellen, executive vice president, D&O and fiduciary liability product leader, FINEX at Willis Towers Watson.

"A mere inaccuracy in a certification could result in criminal enforcement, in which case it would then become a boardroom issue," he said.

A big grey area, however, said Shiraz Saeed, national practice leader for cyber risk at Starr Companies, is determining if a violation is a cyber or management liability issue in the first place.

"The complication arises when a company only has D&O coverage, but it doesn't have a cyber policy and then they have to try and push all the claims down the D&O route, irrespective of their nature," he said.

Jim McCue, financial institutions industry practice leader at Aon Risk Solutions, said many small and mid-size businesses may struggle to comply with the new rules in time.

"It's going to be a steep learning curve and a lot of work in terms of preparedness and the implementation of a highly detailed cyber security program, risk assessment and response plan, all by September 2017," he said.

The new regulation also has the potential to impact third parties including accounting, law, IT and even maintenance and repair firms who have access to a company's information systems and personal data, said Keegan.

"That can include everyone from IT vendors to the people who maintain the building's air conditioning," he said.

NEW MODELS

Others have followed New York's lead, with similar regulations being considered across federal, state and non-governmental regulators.

The National Association of Insurance Commissioners' Cyber-security Taskforce has proposed an insurance data security model law that establishes exclusive standards for data security and investigation, and notification of a breach of data security for insurance providers.

Once enacted, each state would be free to adopt the new law, however, "our main concern is if regulators in different states start to adopt different standards from each other," said Alex Hageli, director, personal lines policy at the Property Casualty Insurers Association of America.

"It would only serve to make compliance harder, increase the cost of burden on companies, and at the end of the day it doesn't really help anybody."

Richard Morris, partner at law firm Herrick, Feinstein LLP, said companies need to review their current cybersecurity program with their chief technology officer or IT provider.

"Companies should assess whether their current technology budget is adequate and consider what investments will be required in 2017 to keep up with regulatory and market expectations," he said. "They should also review and assess the adequacy of insurance policies with respect to coverages, deductibles and other limitations."

Adam Hamm, former NAIC chair and MD of Protiviti's risk and compliance practice, added: "With New York's new cyber regulation, this is a sea change from where we were a couple of years ago and it's soon going to become the new norm for regulating cyber security." **&**

ALEX WRIGHT is a U.K.-based business journalist. You can reach him at riskletters@lrp.com.