Insurers Feel Fresh Heat on Cyber-Security Practices

NY state regulators look at cyber-security practices; 'virtual treasure trove'

By Jaclyn Jaeger

New York state regulators plan to bolster cyber-security oversight in the insurance sector in the weeks and months ahead. Now might be an opportune time for all insurance companies, in New York or not, to review their data security practices.

In March, New York Department of Financial Services Superintendent Benjamin Lawsky said the agency will implement a series of measures to enhance cyber-defenses at insurance companies. These include integrating regular, targeted assessments of cyber-security preparedness at insurance companies as part of the NY-DFS exam process; issuing regulations requiring insurers to meet "heightened standards" for cyber-security; and examining "stronger measures" on third-party vendor representations and warranties.

"Recent cyber-security breaches should serve as a stern wake-up call for insurers and other financial institutions to strengthen their cyber-defenses," Lawsky said. "Those companies are entrusted with a virtual treasure trove of sensitive customer information that is an inviting target for hackers. Regulators and private-sector companies must both redouble their efforts and move aggressively to help safeguard this consumer data."

During remarks delivered on Feb. 25 at Columbia Law School, Lawsky spoke in further detail about the targeted assessments. "The idea is simple: If we grade banks and insurers directly on their defenses against hackers as part of our examinations, it will incentivize those companies to prioritize and shore up their cyber-security protections," he said. "Indeed, institutions care deeply about their examination grades since those scores can impact their ability to pay dividends, or enter new business lines, or acquire other companies."

The scope of these cyber-security efforts will be broad, applying to any company in the insurance sector that does business with New York customers, even if the company is not located in the state. "Many of the big insurance companies are either domiciled in New York, or doing business in New York, so it essentially will affect quite a large group of companies," says Mary Jane Wilson-Bilik, a partner with law firm Sutherland.

The DFS' plans shouldn't come as a surprise to those in the industry. "What they're doing is moving the insurance industry into parity with the rest of financial services companies that already have begun to focus on cyber-security, and build out the risk-management infrastructures they need," says Andy Roth, a partner with law firm Dentons and co-chair of its privacy and security group.

Regulatory expectations aside, insurance companies themselves have a vested interest in cyber-security, since many increasingly write insurance policies to cover cyber-security incidents for their policyholders, says Jason Weinstein, a partner with law firm Steptoe. Given that a cyber-attack on a policyholder creates exposure to the insurance company, "they have a strong interest in ensuring that not only is their cyber-security as good as it can be, but that their policyholders have strong cyber-security measures in place, too," he says.

> "Recent cyber-security breaches should serve as a stern wake-up call for insurers and other financial institutions to strengthen their cyber-defenses."
>
> Benjamin Lawsky, Superintendent, New York Department of Financial Services

Cyber-Security Practices

Lawsky's announcement accompanied a report conducted by DFS on cyber-security practices in the insurance sector. The survey of 43 health, property, and life insurance providers, with combined assets of approximately $3.2 trillion, showed positive results overall for cyber-security preparedness.

According to the report, nearly all insurance providers (98 percent) said they have an information security framework in place that satisfies what DFS considers to be the five essential elements of a robust cyber-security program:

- A written information security policy;
- Security awareness and education and training for employees;
- Information security audits;
- Management of cyber-risk, including the identification of key risks and trends; and
- Incident monitoring and reporting.

All respondents additionally reported using standard "intrusion detection" tools to fight off viruses and hackers. "Insurance companies are doing quite a bit already," says Wilson-Bilik. Where vulnerabilities lie are in vendor management agreements, she says.

Vendor Management

The weak spot among insurers, according to the DFS report, is auditing and monitoring the cyber-security practices of third-party service providers. "In many ways, a company's cyber-security is only as strong as the cyber-security of its third-party vendors," Lawsky said. DFS may even mandate that financial firms receive robust representations and warranties from third-party vendors that they have critical cyber-security protections in place, he warned.

Security risks among third parties are nothing new, nor anything specific to the insurance sector. Likewise, the primary vehicle to police those risks is also well-known: strong language in contracts.

"You need to have contractual terms

that impose obligations on these third parties to maintain a certain level of cyber-security," Weinstein says. The contract also should include terms that give you the right to audit and provide that the vendor will agree to cover your losses in the event of a data breached caused by a vulnerability in their network, he says.

It's also important to require that the vendor immediately alert you to a data breach, "so that you can fulfill your own obligations to notify regulators and the public," Wilson-Bilik says. Ideally, you want the vendor to be certified by an organization like ISO. "What kind of certifications can they provide to you?" she says.

A lot of these contracts were signed before cyber-security concerns came to the forefront. "Even if you have an existing contract with a vendor, it's worth going back and seeing if those contracts adequately protect you," Weinstein says.

Corporate Governance

According to the findings of the DFS report, several departments typically are involved in cyber-security governance, including IT, compliance, risk, and legal. "Bridge the gap between the IT department, senior management, and legal and compliance, because they all have to be in this together," Wilson-Bilik says. "You need to be able to talk the same language."

How often IT security issues get reported to senior management varied across insurers. Only 14 percent of respondents said they update their chief executive officers on a monthly basis. The majority (53 percent) said they update their CEO quarterly, and 60 percent said they also update their CEO when necessary.

Updates to boards are likewise diverse. Most insurers said they update their boards on a quarterly or ad hoc basis, while 14 percent said they provide annual updates. Another 9 percent said they update their boards on both an annual and ad hoc basis.

"Cyber-security is the new normal," Roth says. "That means thinking about how it's governed internally and how issues are escalated to management so that they can have appropriate oversight and control."

Continued on Page 57

CYBER-SECURITY IN THE FINANCIAL SECTOR

Below is an excerpt from a speech by NY Superintendent of Financial Services Benjamin Lawsky on the issue of cyber-security in 2015.

At DFS, we believe that cyber-security is likely the most important issue we will face in 2015—and perhaps for many years to come after that. A question we often get as financial regulators is, 'What keeps you up at night?' The answer is 'a lot of things,' but right at the top of the list is the cyber-security at the financial institutions we regulate.

I am deeply worried that we are soon going to see a major cyber-attack aimed at the financial system that is going to make all of us to shudder. Cyber-hacking could represent a systemic risk to our financial markets by creating a run or panic that spills over into the broader economy. Indeed, we are concerned that within the next decade (or perhaps sooner) we will experience an Armageddon-type cyber-event that causes a significant disruption in the financial system for a period of time—what some have termed a 'cyber 9/11.' And we worry that, when that major cyber-event happens, we will all look back and say, 'How did we not do more to prevent it?'

Of course, the question, then, is: What should we do to help prevent that nightmare scenario? We do not profess to have all the answers at DFS. But we are spending a lot of time working on concrete actions to help strengthen cyber-security at our regulated institutions. In particular, we are focused on ways to incentivize market participants to do more to protect themselves from cyber-attacks. This issue is also clearly at the top of the agenda for federal regulators. Sarah Bloom Raskin, the deputy treasury secretary, in particular has been a leader on these issues.

But I believe this area is one example where, even though federal regulators are very focused on the problem, there is still room for financial federalism at the state level in experimenting with various solutions. Given the magnitude of the problem, we need all the ideas and proposals we can get.

With that in mind, I would like to briefly outline several DFS initiatives in this area. First, we are revamping our regular examinations of banks and insurance companies to incorporate new, targeted assessments of those institutions' cyber-security preparedness.

The idea is simple: If we grade banks and insurers directly on their defenses against hackers as part of our examinations, it will incentivize those companies to prioritize and shore up their cyber-security protections. Indeed, institutions care deeply about their examination grades since those scores can impact their ability to pay dividends, or enter new business lines, or acquire other companies.

Second, we are considering steps to address the cyber-security of third-party vendors, which is a significant vulnerability. Banks and insurers rely on third-party vendors for a broad-range of services—whether it is a law firm that provides them with legal advice or even a company that is contracted to run their HVAC system. Those third-party vendors often have access to a financial institution's information technology systems, which can provide a backdoor entrance for hackers. In many ways, a company's cyber-security is only as strong as the cyber-security of its third-party vendors.

As such, we are considering mandating that our financial institutions receive robust representations and warranties from third-party vendors that those vendors have critical cyber-security protections in place. In other words, those third-party vendors will have to strengthen their cyber-security or risk losing out on business from those financial institutions. That is tough medicine, but we believe it is likely warranted given the risks that cyber-hacking presents to the stability of our financial markets and economy.

Source: DFS.

ABA Seeks Clarity for Corporate Monitors

Continued from Page 16

Goldstock says the ABA also is considering whose responsibility it should be to choose a monitor: "Should a monitor be appointed by a court, an agency, or a prosecutor, or should there be a prequalified pool of monitors from which the host organization has a choice? Should the host organization have a role in determining who the monitor should be?"

Work Plans

The standards also will explore the monitor's obligations for creating a work plan at the outset of a monitorship and further suggest that the work plan be developed in consultation with the host company and government agency. "There needs to be more transparency from the beginning through the end stages," Hanson says.

"From a work plan, you can establish a budget," Hanson adds. That then allows both the company and the monitor to assess more clearly the time and resource needed to carry out the requirements spelled out in the agreement. It also gives the company a better sense of whether the monitor is doing enough, or too much, based upon the framework of the work plan.

"Companies have a right to tell the monitor, 'I want to see exactly what you're doing, how you're doing it. Here are your objectives. Show me how you're going to meet them. We're going to do it not just effectively, but as efficiently as possible,'" he says.

Compensation & Fees

Companies also have a right to transparent practices concerning monitor compensation and fees. The discussion draft suggests that, during the monitor selection and approval process, the monitor should provide a reasonable estimation of fees and expenses that are expected to be incurred to achieve the objectives of the agreement.

> "The standards go a long way toward facilitating a better relationship between the monitor and the company."
>
> John Hanson, Founder, Artifice Forensic Financial Services

From a consulting perspective, a lot of people may view companies that are in hot water with the government as a rich source of fees, Hanson says. "They have no control over what you do. They have to pay you, and you don't even report to them. You can do whatever you want."

Sub-contracting fees are another "big problem area," Hanson says. Some monitors, for example, will charge a flat annual fee—say, $100,000 a year—but fail to mention that the sub-contractors they intend to use come at a cost of another $2 million a year.

Aside from the monitor's work plan, a host company should get a good sense of how much a third-party sub-contractor will be used; what its work plans look like; and what their fees and costs will be.

Evaluation Process

In addition to establishing standards for corporate monitors, the task force went one step further by recommending that the government evaluate the monitor's effectiveness at the end of a monitorship, Hanson says. The idea is to use the results of the analysis to determine whether to consider that monitor again for future assignments and to help government agencies improve the process when designing future monitorships, he says.

"That's easier said than done," Hanson adds. A lot of government agencies, particularly the smaller ones, wash their hands of a settlement agreement once it has concluded, he says.

That is not how most people believe corporate monitorships should be done. "You're not just there to do something, go away, and it all goes back to crap," Hanson concludes. "You're there to help the company make a big change, so that they can stay out of trouble in the future and be a better organization." ■

Insurers Feel Fresh Heat on Cyber-Security Practices

Continued from Page 21

In its report, DFS further stressed the importance of taking part in information-sharing groups as a way to be aware of the latest threats and vulnerabilities affecting the industry. "The department believes that institutions of all sizes can reap benefits from membership in information-sharing organizations, such as the Financial Services-Information Sharing and Analysis Center (FS-ISAC)," DFS said. "Members of FS-ISAC receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber-security threats."

Moving Forward

So how can IT, compliance, and risk professionals in the insurance industry best prepare for a DFS-targeted cyber-security assessment?

Cyber-security experts say one good starting point is to take a look at the guidance that DFS issued for banks in December that identified specific issues and factors it would examine in the course of targeted, cyber-security preparedness assessments. These topics include protocols for the detection of cyber-breaches, penetration testing, corporate governance related to cyber-security, defenses against breaches (including multi-factor authentication), and security of their third-party vendors.

"Bolstering cyber-security in the financial services industry has been, and will continue to be, a high priority for the department," DFS warned. "Just as the institutions regulated by the department are encouraged—and expected—to stay current on the changing landscape of cyber-security, the department plans to do the same." ■