Getting in Line with the New Regulations

Cybersecurity rules from the New York Department of Financial Services are broad and complicated

__Michelle Reed__, a litigator at __Akin Gump Strauss Hauer & Feld LLP__ and co-leader of the firm's cybersecurity privacy and data protection group, breaks down what the New York Department of Financial Services' new cybersecurity regulations mean for covered entities and the in-house counsel who advise them. Her remarks have been edited for length and style.

The New York Department of Financial Services (NYDFS) recently revised its cybersecurity regulations for covered entities, with compliance required as early as February 15, 2018. Who will be impacted and how?

Michelle Reed: The NYDFS cybersecurity regulations are really the first of their kind nationwide. The regulations apply to covered entities: state chartered banks, licensed lenders, private bankers, mortgage companies, insurance companies and other service providers. There are certain exemptions, but they're pretty limited.

The regulations were effective in March of this year, and many of the requirements actually needed to be adhered to as of August 28. That means by August 28 each covered institution had to adopt a robust cybersecurity program. NYDFS provides solid detail of what it expects in that cybersecurity program. For example, you need to identify your cybersecurity threats. Companies need to employ defense infrastructure that would protect against those threats. They need to have a system to detect what's happening and a system to respond. Once companies respond, they have to fulfill different regulatory reporting. People who work in the cybersecurity industry are going to be familiar with this because it parallels the National Institute of Standards and Technology's cybersecurity framework.

There's an expectation that any organization will have this robust cybersecurity program and a comprehensive cybersecurity policy. This policy is specifically going to cover information security, access control (who has access to what and how) and disaster recovery in the event of a total system shutdown or a ransomware attack (so that your company can get back up to speed). It also requires that companies have policies regarding systems – network security and data privacy. And then, most importantly, that they provide regular risk assessments. All of these policies needed to be adopted by August.

NYDFS expects a qualified chief information security officer (CISO) to oversee and implement the cyber program. Many companies may have a chief information officer or network security administrator who's filling that role, but they don't actually have a CISO designated. Third parties can also be hired to fill this role.

Additionally, NYDFS has an expectation that personnel will be trained to manage through these various cybersecurity risks. And companies are expected to notify the NYDFS of all material cybersecurity events. For those that carry a reasonable likelihood of causing material harm, companies also have to limit access privileges. They should make sure that privileged access is not being given to a wide variety of users, but instead access is very limited. In a breach situation, privileged access can often determine how extensive the damage will be. These are the requirements that need to be addressed by August 28.

What are the exemptions to the revised regulations?

Reed: There are not many, but if you're a small company, there are some. A covered entity with less than $5 million in gross annual revenue in each of the last three fiscal years, fewer than 10 employees or less than $10 million in year-end assets total is exempt. A company that is an employee agent, representative or designee of a covered entity that itself is covered by the cybersecurity program is exempt. So is an entity that does not operate, maintain, utilize or control any information or does not control, access, generate, receive or possess nonpublic information. But they must be rare because virtually every company has some kind of nonpublic information that is going to require protection.

The other piece that I think is important is that the rules allow for some assessment of your own entity, and when you did your cybersecurity risk assessment, they allow for some scaling based on what it showed. That doesn't mean that your company is exempt, but there is some flexibility with certain requirements. For example, Section 500.12(b) on multifactor authentication says that a company can use a different method to control access to data if the CISO makes a specific finding that the alternative method is a reasonably equivalent arrangement.

Who are the enforcement officials for these regulations?

Reed: Ultimately, you're going to be dealing with the NYDFS, Financial Frauds and Consumer Protection Division (FFCPD) and potentially the state attorney general, depending on the issue.

If you say, "I don't fall under one of these covered entities, and I'm not subject to the NYDFS, so I don't need to worry about any of this," my recommendation is to take a step back and ask, "What am I subject to?" You do business across the United States. There are varying state laws and regulations that address some of these requirements. Companies need to know where they are operating and what the applicable standards are. Most states have notice requirements, as opposed to technical cybersecurity requirements like NYDFS, but in that case, your company is subject to any state attorney general in the United States. If you're an international business, you'll soon be dealing with the EU's general date protection regulation (GDPR). There are many technical requirements and notification obligations associated with that – and subject to the data protection authority (DPA) in the various European countries.

Do you think the New York threshold is higher or lower than the GDPR standards?

Reed: I wouldn't characterize it as higher or lower; it's just different. There are probably aspects that are more rigorous, but there are aspects that are not. Some of the privacy by design requirements in GDPR are significant, but the New York standard also contains significant responsibilities; for example, encryption. The base level expectation is that you're encrypted in transit, encrypted at rest. That's a significant requirement that requires a real investment from companies and can impact day-to-day operations. The reality is that both of these regulations demonstrate that regulators are going to take a more detailed, compliance-heavy approach with cybersecurity than they have in the past.

The regulations require entities to "establish a written incidence response plan designed to promptly respond to and recover from any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entities business or operations." Would you talk about the materiality threshold?

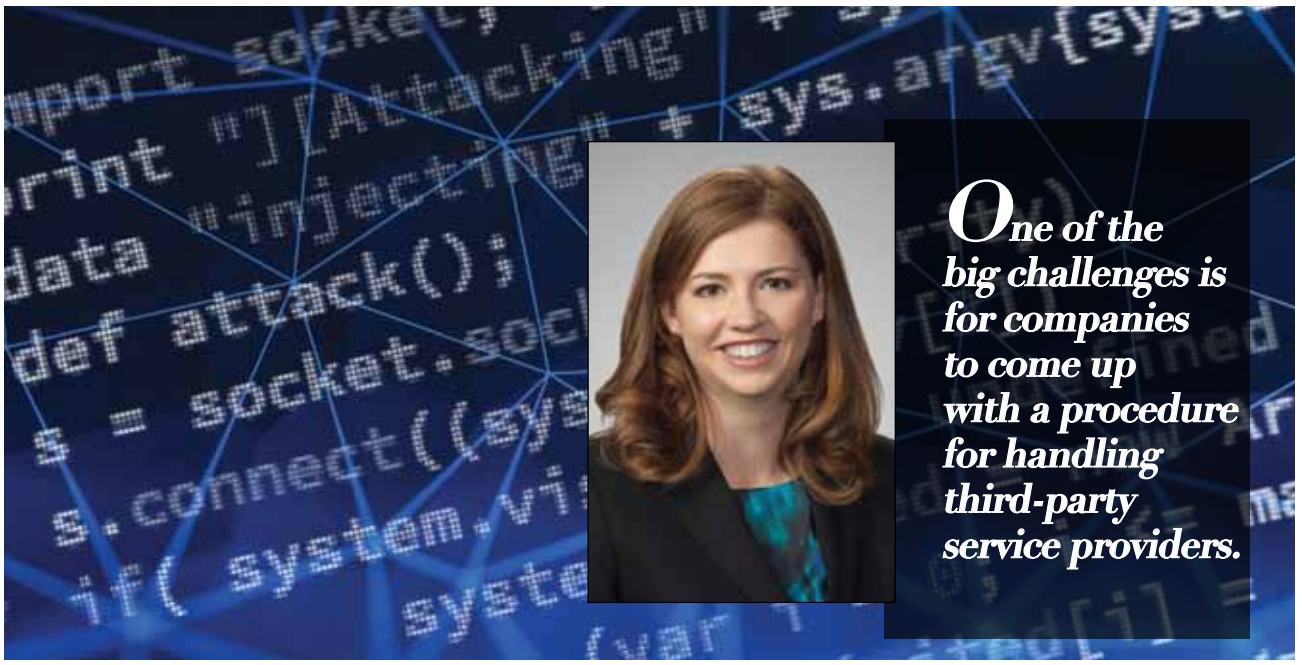
Reed: This materiality threshold is going to be a bit of a moving target in terms of understanding what is going to require reporting and what is not. Those who don't deal with cybersecurity regularly think, "Well, it's simple. You have an event and therefore you report it." What people don't realize is that a lot of these companies are experiencing thousands of events a day, of varying success levels.

Evaluating what is material is important for an in-house lawyer and sometimes requires seeking outside counsel's advice in determining what materiality means. There are lots of contexts in which we assess materiality, but in general, something material is not trivial. Under securities laws, you look at the total mix of information, then characterize it based on the risk of harm and likelihood of occurrence of that harm.

For example, if you had an event that was a low likelihood of occurrence but a high degree of harm, you may find that material. On the flip side, if you have something that is highly likely to occur, but it's not going to impact the company at all, then a lot of times you consider that not to be material. To apply that to the cybersecurity context, you want to look at events that happened and ask questions. What happened? Did they gain access to information? Did they gain access to credentials? Was any information exfiltrated? If it was some sort of Distributed Denial of Service (DDoS) or ransomware attack, how did that harm our website availability for business or our ability to conduct business if our systems were encrypted? Once you consider all of the information from a particular attack, it becomes clearer whether something is trivial or not trivial, material or immaterial.

One of the tricky parts of the NYDFS regulations is the requirement for reporting if there's a cybersecurity event that had a reasonable likelihood of materially harming any material part of normal operations of a covered entity. This is difficult because it is

Michelle Reed *is a litigator at Akin Gump Strauss Hauer & Feld LLP and co-leader of the firm's cybersecurity, privacy and data protection practice. She specializes in advising clients on data breach investigations, notifications and subsequent litigation. She can be reached at mreed@akingump.com.*



assuming that the attack was not successful. A lot of people would ask, "If an attack was not successful, how can that be material?" This goes back to the likelihood of occurrence and the magnitude of harm. If you have an attack that wasn't successful but could have a significant impact on your business, that may be required to be reported under section 500.1782 of the New York regulations.

A question that's going to evolve over time is an attack that may be material now might not be in a few years, depending on what our resources are and our abilities are to protect against it. It helps to talk to someone who has been through this so that they can evaluate whether or not something is material for the purposes of reporting.

What are the implications in terms of training to execute an incident response plan?

Reed: There is not a great way to implement an incident response plan without testing it. You really need to test it and train the people who are designated to respond so that they know what they're doing. I work with clients to establish incident response plans. We come up with what we think is going to be a good fit for a particular company, and there isn't an incident response plan that you can take from one company and drop into another because companies operate so differently. We'll think the plan is great, and then we'll test it. We'll do a tabletop exercise where we come up with a hypothetical scenario and run through a breach. We gather the team, figure out how they're going to respond, and in connection with that tabletop scenario, discover we hadn't thought about this question, that question and the other question. Maybe an employee doesn't even know how to report the incident, you don't have an incident response hotline or you don't have a clear establishment amongst your employee base on how to report the incident. Maybe you don't know at what threshold to report up to the board. Maybe your information security team doesn't have proper authority to shut down a ransomware attack fast enough. Maybe PR wasn't looped in to begin with and then issued inconsistent statements or otherwise wasn't consulted early enough to frame the response. There are so many different problems that happen with incident response.

Stepping back and evaluating that by going through your hypothetical scenario will ultimately make your response to an actual breach infinitely better. Every company at some point will have a data breach. The way it is going to be judged by the regulators, by its customers, by its employees is going to impact its long-term public relations battle, its regulatory battle and ultimately its legal position in the ongoing litigation. How you respond matters, and investing in testing matters.

What is the in-house lawyer's role in cybersecurity for covered entities?

Reed: The regulation doesn't explicitly state that there are obligations for the in-house attorney. When you evaluate the regulation, however, it becomes very clear that in-house attorneys play a critical role in helping frame and provide follow-up for the cybersecurity protections of various financial institutions. It is important for the in-house lawyer to take the lead in making sure that there is compliance. So the lawyer is going to want to look at things like incident response. Do we have a plan? What is my role as an in-house attorney in responding to incidents? Breech notifications – what are we going to do if we have to notify? Do we know what our contractual obligations are? Do we know what our statutory obligations are? Vendor management is a huge part of an in-house attorney's job, and I think a big headache for a lot of them. In-house lawyers constantly deal with third parties and vendor contracts. What are the requirements for those vendors, what audits have been done in connection with that and what follow-ups are critical for the in-house attorneys to understand and to encourage?

Then, of course, there's compliance. You can have policies all you want, but if you're not complying, it ultimately doesn't get the company where it needs to be from a cybersecurity standpoint. The in-house lawyer plays a critical role in helping ensure that a company is compliant with the policies that have been adopted.

What do the revised regulations state about breach notification, and how can in-house lawyers navigate the various breach notification rules?

Reed: The current regulations set forth a materiality standard for reporting within 72 hours of the determination that the event requires notice to any government body, self-regulatory agency or other supervisory body or has a reasonable likelihood of materially harming any material part of the normal operations of the covered entity. In the data breach world, 72 hours is a really short time line.

That doesn't mean that if you have a breach and you realize there is a problem, it's 72 hours from the time someone told you, "We may have bad guys in our system." That's not the rule. The rule is 72 hours from the time you've made a determination that you may have to provide notice. That gives you some time. Why does that make a difference? Because typically, the notice provisions are going to be triggered by what data was taken or accessed. If the data contained nonpublic personal information, then you're likely going to have a reporting duty.

But it can be difficult to know when the decision that notification would be required was reached. You have to have someone who is familiar with the rules and the decision-making process on when to notify, how you determined it, how you determined what data was accessed, how you determined if it was a successful breach or an unsuccessful breach. These are technical questions but also legal questions. That's why the in-house attorney has a substantial role in making that happen and making that determination.

The revised regulations call for written policies and procedures designed to ensure the security of information accessible to or held by third-party service providers. How can in-house counsel best achieve compliance with this portion of the regulation?

Reed: In my opinion, this is one of the hardest things to implement for a company. Most financial services companies of any size are pretty sophisticated in their cybersecurity governance and their cybersecurity policies. What is really challenging is for companies to come up with a procedure for handling third-party service providers. For this reason, the regulations give two years for compliance with this piece. I think the regulators recognize that this is going to take a long time to get in order, so this is not required until March 1, 2019.

Lawyers should be looking at helping develop third-party management programs. Make sure that you know where your contracts are, that you conduct ongoing diligence, and that you documented it. A big pitfall for a lot of companies is that they do due diligence when they bring on a new vendor, then never do due diligence again. Negotiate contractual provisions that address issues with respect to cybersecurity – access control, encryption, warranties on policies and procedures related to cybersecurity – and of course and importantly, notification of cybersecurity events. Under these new regulations regarding vendor management, you want to make sure that you have explicitly contractually provided for the data breach notification and security obligations so that you can comply with your own procedures and the NYDFS regulations.

What do covered entities need to know about data retention, encryption and multifactor authentication?

Reed: With respect to data retention, covered entities must have policies and procedures for disposal of nonpublic information that's not needed for business operations or other legitimate business purposes. I'm so happy that they put this in there because the best way to protect yourself against a cyber event is to have less data. Some of the worst things that come out of data breaches are not necessarily current data. It could be data from a long time ago that can make quite a public splash once it's made public by hackers.

The regulations require multifactor authentication only for individuals accessing internal networks from an external network. The CISO would have to approve reasonably equivalent or more secure access controls to opt out.

On encryption, you're going to have encryption requirements for data in transit and at rest. And that's going to cause some growing pains for lots of companies.