Cybersecurity Takes Center Stage

New York's new law establishing mandatory digital-safety protocols is part of an expanding regulatory push

By Al Alper

Earlier this year, the state of New York adopted the "first-in-the-nation" set of cybersecurity compliance requirements that specifically impacted any businesses or organizations that report to the state's Department of Financial Services (DFS). Known officially as 23 NYCRR Part 500, and enacted on March 1, 2017, the 180-day transitional period for the regulations recently ended — on Aug. 28 of this year.

Affected businesses should have now met the first round of robust cybersecurity requirements. While any mortgage professional working in the state of New York will almost immediately be affected by the new law, mortgage professionals nationwide also should pay attention to New York's new mandates.

Businesses in nearly every industry face new and expanding cyber threats, so other states already are monitoring New York's actions and may consider adopting similar requirements to safeguard personal and financial data.

Photo illustration by Karen Steichen

New York law

If you are a New York-based business that reports to the state's financial regulator, DFS, you should, by now, be in compliance with the following:

- Establish and maintain a cybersecurity program;
- Implement and maintain cybersecurity policies and procedures that protect nonpublic information;
- Designate a qualified individual (internal or outsourced) to serve as chief information security officer;
- Establish an audit trail, determine access privileges and implement application security;
- Identify cybersecurity personnel and intelligence, and develop a third-party service-provider security policy;
- Devise limitations on data retention, establish training and monitoring programs, and ensure the encryption of nonpublic information; and
- Ready an incident-response plan.

New York businesses and organizations subject to the new law also should have — by Sept. 27 of this year — filed a notice of exemption if they determined they might be excused from any of the cybersecurity requirements. The limited exemption criteria include thresholds for total number of employees, gross revenue and year-end total assets. If a business or organization falls under these exemption thresholds, it will get relief from some of the requirements, but not all.

Continued >>

Al Alper is CEO and Founder of Absolute Logic (www.absolutelogic.com) and CyberGuard360 (www.cyberguard360.com). Since 1991, Absolute Logic has been providing Fortune 500-style technical support, security services and technology consulting to businesses of up to 250 employees within Connecticut and New York. Alper also is a national speaker on information-technology and security issues, and has authored the popular books, "REVEALED! The Secrets to Hiring the Right Computer Consultant" and "REVEALED! The Secrets to Protecting Yourself from Cyber-Criminals." Reach Alper at al.alper@absolutelogic.com or (855) 255-1550.

Scotsman Guide

Reprinted from *Scotsman Guide* Commercial Edition and **ScotsmanGuide.com**, November 2017

<< Continued

Broader impact

Given the wide array of New York industries affected by the new cybersecurity requirements — including commercial and residential real estate financing professionals, such as mortgage bankers, mortgage brokers, mortgage originators and mortgage loan servicers — this isn't, and shouldn't be, just a New York issue. Other states have been or are starting to implement their own digital-security regulations — including most recently Colorado, which this summer adopted new cybersecurity guidelines that apply more specifically to broker-dealers purchasing securities in Colorado — as well as investment advisors who do business in the state.

■0In fact, since 2002, 13 states have enacted some kind of state regulations on cybersecurity, and it's almost a certainty that more states will follow these and develop their own regulatory framework. On the federal level, the National Institute of Standards and Technology (NIST) in 2014 published a voluntary framework for helping groups manage cybersecurity risks related to the country's critical infrastructure. That effort, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, has seen wide acceptance throughout many industries and organizations. This past January, a newly expanded draft update to the Cybersecurity Framework was released.

■0While some sets of cybersecurity guidelines now in existence are much more limited in scope than the New York state directives, the trend in cybersecurity protection is that states are expanding their regulatory reach and the range of industries subject to such protocols. And why not?

■0For mortgage professionals in particular, and for other finance professionals who have access to individuals' personal and/or sensitive information, evaluating your organization's cybersecurity posture just makes good business sense. Businesses in virtually every industry face new and continually more sophisticated threats from cybercriminals. Many of the mandated steps laid out in New York's 23 NYCCR Part 500 requirements are just best practices that aren't terribly expensive or too difficult to employ. A qualified information-technology (IT) or technology-security company can help put them in place quickly and easily.

Business concerns

As you review your cybersecurity needs and determine how to move forward to safeguard your technology, you will want to review your IT capabilities and identify any potential exposure. Aside from ensuring compliance with any state regulations you may face, this kind of internal assessment also is a great way to ensure that your organization is doing all it can to protect clients' sensitive information.

After all, regardless of compliance issues, a cybersecurity breach has the potential to cause your business serious damage in the form of lawsuits and significant loss of business. Additionally, your ability to promote what you're doing in terms of protecting your clients' data could be a market differentiator.

For owners of smaller businesses without internal IT capabilities, look to partner with an IT security provider who can offer a turnkey solution that offers a package of cybersecurity services to meet all the requirements. IT security providers who are knowledgeable about the comprehensive 23 NYCCR 500 requirements may be able to offer your organization better overall guidance for current and, potentially, future state and federal regulations.

Midsize companies can benefit as well from partnering with a similarly informed IT security provider who can offer advice on comprehensive cybersecurity protection. Even larger companies might find that working with an outside IT security partner can help them fulfill one or two integral elements of a broader cybersecurity plan through a la carte options.

■ ■ ■

As the NIST continues to update and expand its recommendations, and more states enact regulations focused on cybersecurity, mortgage professionals throughout the country would do well to look to the comprehensive New York State guidelines as a model to help ensure their companies' — and their clients' — data are protected. Although the specifics can be potentially confusing from state to state, the overarching theme of cybersecurity protection is one that everyone can get behind. ■