# Cybersecurity Isn't a Luxury Item

## Mortgage professionals share responsibility for ensuring their clients' private digital data is protected

By Al Alper

One of the last things mortgage professionals would ever want to do is put their borrowers' personal information at risk as part of the lending process. The consequences of a malicious digital breach can be devastating for mortgage companies and their clients.

The risk of such a data compromise is very real, given all of the moving parts mortgage professionals deal with on a daily basis. That reality, combined with the amount of financial data and other personal information the industry requires to advance the loan process and secure funding, makes cybersecurity an ever-present demand.

Although mortgage professionals working for large companies may not face the same data risks as those at smaller enterprises with fewer resources, they still should ensure they're complying with their company's cybersecurity policies. That includes bringing any potential cracks in that cybersecurity armor to the attention of those responsible for addressing the problem.

While it's important to keep in mind that mortgage companies of all sizes are at risk, smaller companies, in particular, may be more vulnerable. In fact, in 2016, about half of all internet attacks worldwide targeted companies with fewer than 250 employees. If anything, the idea of thinking that your company is too small to become a cyber victim might just increase the likelihood of it becoming one.

### Scrutiny increasing

Over the last several years, state and federal governments have played an increasing role in thwarting cyberattacks. In fact, October 2017 marked the 14th anniversary of National Cyber Security Awareness Month, an initiative originated by the U.S. Department of Homeland Security and the National Cyber Security Alliance.

It was created as part of a collaborative effort between government and industry to ensure all citizens have the resources needed to stay safer and more secure online while also protecting their personal information. By collaborating on cybersecurity, government and the private sector can each focus on their strengths in the cybersecurity realm, and then share their combined knowledge for the benefit of both sectors to improve their cybersecurity responses.

The federal government, for example, has formidable resources to identify and interpret potential cyber threats around the globe, but it isn't necessarily the best at distilling this data and quickly creating protective measures. The private sector, on the other hand, couldn't compile this trove of data on its own, but can make much better sense of it and use that information to develop next-generation tools.

### States responding

Recently, we have seen states take matters into their own hands when it comes to protecting their residents from becoming victims of hacking and other cyber crimes. New York's first-in-the-nation set of cybersecurity-compllance requirements went into effect on March 1, 2017. The regulations affect any company that falls under the oversight of the New York Department of Financial Services (DFS), and that includes the mortgage industry.

The requirements of the new law — 23 NYCRR Part 500 — include the following mandates:

- ■ **Establishing** and maintaining a cybersecurity program;
- ■ **Implementing** and maintaining a cybersecurity policy;
- ■ **Designating** a qualified individual (internal or outsourced) to serve as chief information security officer (CISO);
- ■ **Limiting** user-access privileges as part of the cybersecurity program;
- ■ **Utilizing** qualified cybersecurity personnel;
- ■ **Establishing** a written incident-response plan;
- ■ **Notifying** the DFS of cybersecurity events as required; and
- ■ **Filing** a notice of exemption from the law, if applicable.

Mortgage professionals who fall under this regulation need to act quickly to ensure that they are prepared to comply with the law and its various mandates and deadlines. Fines will be fast and heavy for organizations that are found to be noncompliant.

Chief information security officers, or CISOs, for example, were required to deliver an annual report to the board or governing body of their respective companies by March 1. In addition, companies subject to the full regulations must begin conducting annual penetration testing, biannual vulnerability assessments and periodic risk assessments. They also must establish multifactor authentication, if needed, and provide regular cybersecurity-awareness training for all personnel.

Continued >>

**Al Alper** is CEO and founder of Absolute Logic (absolutelogic.com) and CyberGuard360 (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. Absolute Logic was named a National Cyber Security Awareness Month 2017 Champion. Alper is also a national speaker on information technology and security issues. Reach him at al.alper@absolutelogic.com or (855) 255-1550.

Scotsman Guide

Reprinted from *Scotsman Guide* Commercial Edition and **ScotsmanGuide.com**, March 2018

<< Continued

The state of New York is not alone in taking serious steps to thwart cyber threats. More than one in five states have already enacted some version of cybersecurity regulations, and that number is poised to grow.

## Foundation building

Regardless of whether you're working for a mortgage company scrambling to meet regulatory deadlines in a state that has a law in place, or a commercial mortgage broker somewhere else in the country, cybersecurity threats are a real and omnipresent danger. Consequently, it's crucial to do everything possible to ensure your company — and your clients — do not become the latest cyber victims.

Lending organizations in every state should be implementing cybersecurity initiatives that protect against hackers, especially given that many of these strategies don't cost a lot of money. In fact, developing a work environment focused on cybersecurity, combined with the appropriate ongoing training, will potentially save a company money and time associated with recovering from a data hack.

Even simple steps matter, like requiring longer, more complex and frequently changed passwords; setting up 10-minute screen savers; establishing individual logins; devising backup and disaster-recovery plans; and facilitating ongoing training. All these measures contribute to creating a foundation for a much more secure operating environment.

■ ■ ■

As a mortgage professional, your clients are putting their hopes, dreams and financial future in your hands, while cybercriminals are constantly becoming more sophisticated in their attacks. It's imperative that you do all you can to protect your borrowers from that threat. Beyond being good business sense, and regardless of state mandates, it's simply the right thing to do. ■