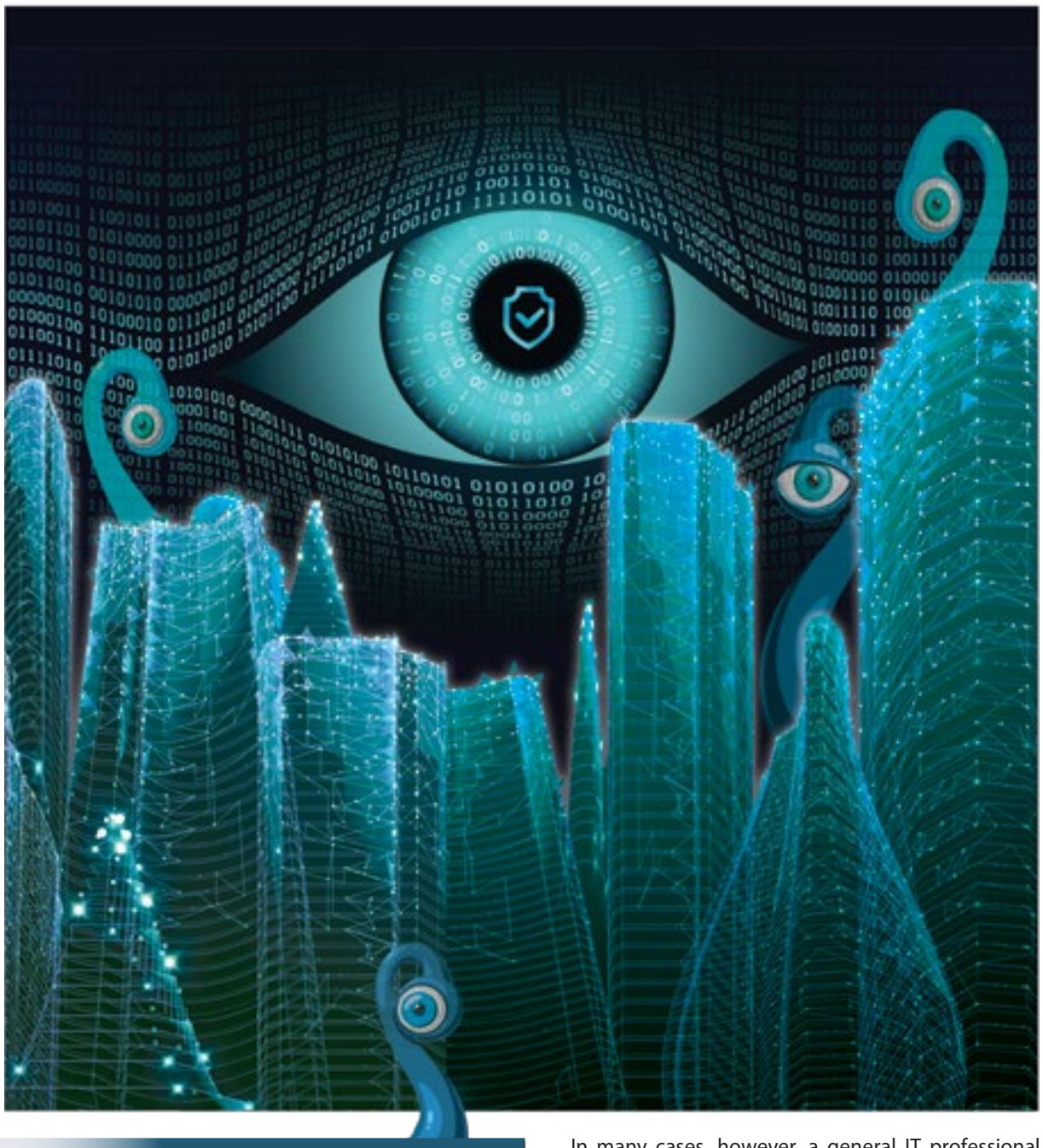
View Cybersecurity From All Angles

Improve data safeguards with technical tools, traditional methods and training

By Al Alper and Mark Favaloro



It is not news that commercial mortgage brokers and lenders need to pay close attention to cybersecurity issues. Financial institutions store an immense amount of sensitive personal information from borrowers, and remain prime targets for hackers and cybercriminals.

Aside from protecting themselves and their borrowers from the potentially crippling losses that accompany a data breach, commercial mortgage brokers and lenders have another reason to pay close attention to cybersecurity. The government has taken notice of the threat.

In the near future, most states and the federal government will likely pass regulations that require financial-services companies to implement cybersecurity measures. Two of the nation's biggest states — New York and California — already have passed cybersecurity laws that could become a model for federal regulations. New Jersey also has pending data-privacy and cybersecurity legislation.

New York's rules, which were originally implemented in 2017 and are now fully phased in as of this past March, established requirements for all companies that report to the New York State Department of Financial Services. These regulations affect nearly the entire mortgage industry. New York's rules require companies to assess their risks and implement a plan that proactively addresses those risks. This serves as a harbinger of things to come on the national level. Additionally, the General Data Protection Regulation enacted by the European Union in May 2018 also could offer the U.S. government some guideposts on how to implement cybersecurity measures nationwide.

Cybersecurity regulation is expected to remain a front-burner issue through 2019. There is a good chance that new laws will be passed in 2020. At a minimum, the interest shown by government officials toward cybersecurity issues should be taken as a sign that companies will soon be required by law to address the threat.

To prepare your commercial mortgage company for future regulation, and to protect your company's and clients' best interests, it's imperative to recognize that cybersecurity requires a comprehensive and multifaceted approach. Mortgage companies need to address the threat via a three-pronged approach that includes the use of technical tools, traditional methods of safeguarding physical files and employee training.

Technical strategies

Cybersecurity requires specialized technical expertise. Step one is to hire a cybersecurity professional. Mortgage companies most likely have their information technology (IT) needs covered by an in-house team, or through an independent IT professional or service provider.

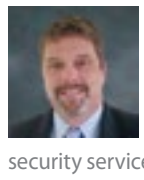
In many cases, however, a general IT professional will not be fully able to meet a company's cybersecurity needs. Regardless of what state laws mandate, a regular IT professional will most likely not be schooled in the levels of cybersecurity needed to truly protect all aspects of the business.

Continued on Page 80 >>

Key Points

Implementing a cybersecurity plan

- **Hire a cybersecurity professional with specific technical expertise.**
- **Encrypt all inbound and outbound e-mails.**
- **Consider multifactor authentication, firewalls and other software protections.**
- **Set up physical security procedures, such as locking doors and file cabinets.**
- **Train employees on responsible usage of social media.**
- **Purchase liability insurance to shield your company from successful cyberattacks.**



Al Alper is CEO of Absolute Logic, Inc. (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 can be reached at al.alper@absolutelogic.com.

Mark Favaloro is president of the New York Association of Mortgage Brokers, and is a licensed mortgage loan originator and principal of Aamtrust Mortgage. He can be reached at mfavaloro@aamtrust.com.

<< Cybersecurity continued from Page 78

Your cybersecurity professional should be well-versed in state-specific cybersecurity regulations. After all, if you're doing your due diligence to protect your company's and your clients' data, you want to make sure you do it the right way to maintain compliance.

Companies need to implement tools that will protect their systems from an attack. Encryption should be installed to deal with all incoming and outgoing messages. Encryption scrambles the text of a file in such a way that only authorized parties can read it. Multi-factor authentication — in which the user must present more than one piece of evidence to prove their identity and access data — also should be an available tool.

> **"Despite a company's best efforts, an employee can still fall victim to a hacker's trap."**

Firewalls and other software protections are a must, especially to avoid "shadow IT" breaches, which occur when hackers use bots and other technologies to get into a system. Transaction-based financial institutions with many participants involved in each transaction, including commercial mortgage companies, are especially vulnerable to these attacks.

Securing the office

Cybersecurity plans also must include traditional measures of securing the office to protect information and documents. In this respect, cybersecurity resembles traditional security. A mortgage company should do a careful assessment of the layout of its building to help establish adequate policies.

These policies should set down specific rules, such as who locks the doors at night; whether file cabinets should remain locked and who has access to the filing cabinets; whether cameras should be installed throughout the office and, if so, where they should be placed; and so on.

These types of actions are meant to prevent a casual visitor from accessing physical files. A visitor may, in fact, be a hacker looking for information in plain sight to steal. Securing the office is not meant to instill fear in your employees, but it may discourage employees from a latent attempt to take advantage of the company.

Training employees

In an era when much communication is done online, employees can inadvertently expose their employer to a cyberattack. A company needs to adopt policies and train employees on the use of social media, their personal devices, and their access to and responsibilities in handling company files. Employees, for example, should clearly know what they are allowed to post on social media, and they should be reminded to not open suspicious e-mail attachments.

A company should strive to create an environment where employees discuss the risks of cyberattacks and can learn from each other. This training doesn't have to be time-consuming or overwhelming. Rather than holding monthly, day-long training sessions that put everyone to sleep, plan instead to conduct quarterly reviews of policies. The training also may come via routine security announcements in staff-meeting agendas, messages on pay stubs and login popups. Managers may include a discussion about cybersecurity during the employee's annual review.

Despite a company's best efforts, an employee can still fall victim to a hacker's trap. Mortgage companies can further protect themselves by investing in a liability-insurance policy that shields the company in the event of a cyberattack. Cybersecurity is far from being a one-dimensional issue, and mortgage professionals need to approach cybersecurity from all angles, including the technical, physical and human dimensions. ■