Lurking Hackers Everywhere

Mortgage companies must remain diligent to prevent information-security breaches

By James M. Deitch

Information-security risks have evolved dramatically over the past several years. Malware, or software designed with the intent to steal, damage, disclose or destroy data, has evolved even faster. Hackers have become more sophisticated, and hacking tools have become dramatically more advanced and available.

Mortgage companies have significantly more exposure to information-security risks than many other businesses, and not just from external hackers. Threats lurking inside your own company and regulatory mandates descending like a hammer add to a mortgage company's hacker headaches.

Three areas in particular place mortgage companies at a much higher risk for bad consequences from information-security breaches than typical businesses face: hacker threats, employee and insider threats, and regulatory threats. Of the three, hackers tend to grab the most headlines, because they often crave publicity and their crimes tend to be sensational in terms of the footprint of malicious damage done.

The National Institute of Standards and Technology (NIST) outlines five core functions for an effective information-security program — identify, protect, detect, respond and recover. These terms are used to help describe the intent of the specific security practice.

The core functions of identify, protect and detect are important with an outside sales force. Many hackers know that some mortgage lenders use outside originators — and these originators often use vulnerable Wi-Fi connections in Realtor offices, businesses, coffee shops and other unsecure locations.

Many mortgage companies also allow originators to use their own laptops, tablets, smartphones and other devices. This policy presents a variety of information-security risks, including the use of a variety of nonstandard devices that the lender cannot fully control.

The large number of branch offices where data is collected, used and stored also requires

Continued >>

James M. Deitch is CEO and co-founder of Teraverde Management Advisors. Deitch is a thought leader, author and speaker in the mortgage-banking industry, having served as CEO of four community banks over 25 years. He is a certified mortgage banker and has extensive sales, operating and capital-markets experience. He has authored many articles on information security, and recently released a book, "Hacked. Screwed. Gone," available through Amazon and other booksellers. Reach him at jdeitch@teraverde.com.

Scotsman Guide

Reprinted from *Scotsman Guide* Residential Edition and ScotsmanGuide.com, August 2016

All rights reserved. Third-party reproduction for redistribution is prohibited without contractual consent from Scotsman Guide Media.

<< Continued

all of NIST's core functions to be addressed, including the following:

- **Identify** the information-security risks;
- **Protect** data and availability of information systems;
- **Detect** hackers or the unauthorized exfiltration of data;
- **Respond** to hackers or unauthorized exfiltration of data; and
- **Recover** from any security incident to resume normal operations.

Employee threats

The 2015 Verizon Data Breach Investigations Report found humans and users account for 90 percent of cybersecurity incidents, and many of those are a direct cause of social-engineering attacks. These tactics trick employees into opening e-mails, visiting websites, permitting physical access, or plugging thumb drives or other media into lenders' computers for the purpose of inserting malware, gaining unauthorized access or both.

Organizations' multiple layers of hardware and firewalls can be compromised by a social-engineering attack activated by employees or vendors who are undertrained or not diligent. Even the best network security can be bypassed when lenders' employees or vendors are tricked by a social-engineering attack and allow attackers in by their actions.

Training and testing employee susceptibility to social engineering usually does not get the resources that may be appropriate in many mortgage companies. Social-engineering susceptibility and focused individual training for all employees can be cost-effective at reducing information security threats. Research from the Aberdeen Group shows that susceptibility decreases by as much as 70 percent after appropriate training, testing and recurrent training.

Originators and other employees who deal with customers are at heightened risk of social-engineering attacks. Hackers can target originators, processors and underwriters with a variety of techniques, including phishing e-mails containing attachments with a malware payload.

Many companies have experienced "ransomware" incidents introduced by originators and branch managers. Ransomware encrypts data and then demands a cash ransom to unlock the computer. In some cases, entire servers have been encrypted. Imagine being unable to access your servers and computers at the end of a busy month of scheduled loan closings.

Regulatory threats

As if losses from fraud are not enough, regulatory action is a real threat. This past March, for example, the Consumer Financial Protection Bureau (CFPB) assessed a $100,000 penalty against Dwolla, a consumer payment-processing company.

The CFPB charged Dwolla with making claims about information security on its public website and to customers that weren't fully accurate. As part of the enforcement, Dwolla must train employees on the company's data-security policies and procedures, and on how to protect consumers' information. Dwolla also must fix any security weaknesses found in its web and mobile applications, and securely store and transmit consumer data.

Lenders that do not monitor the removal of data from corporate systems also are at extreme risk to a variety of threats. Alleged misdeeds by originators or branch managers can cause significant liability, as Guaranteed Rate discovered. This past March, a California jury ordered Guaranteed Rate to pay $25 million in damages to Mount Olympus Mortgage. Mount Olympus alleged that a former employee defrauded the company by taking several active loan files and borrower data to his new position at Guaranteed Rate, although Guaranteed Rate denies the allegations.

The California attorney general's Breach Report this past February stated the following: "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet." Companies that fail to implement the applicable controls, the report continues, have a lack of reasonable security.

These 20 controls, suffice it to say, are robust, and failure to properly implement them could create the presumption of a lack of reasonable effort. Such a lack of effort could open a company up to significant enforcement actions.

Stop the threats

So, what are mortgage companies to do to minimize cybersecurity risk? There are three main defenses: employee training and awareness, appropriate information-security controls and the "tone at the top."

Companies should undertake a social-engineering test to assess their susceptibility to these types of attacks. Based on the results, employees can complete specific training modules based on their level of susceptibility. Continued testing and follow-up training demonstrate a company's commitment to increasing employee awareness of social-engineering schemes. This training and testing also should be performed on all newly hired employees.

Monitoring technology may be used to oversee activities on all employees' computers and report any activity that is suspicious, such as downloading hundreds of megabytes of data. Certain employee or vendor activities may indicate that loan applications or other data are being diverted for unauthorized use.

Mortgage companies also need to focus on developing an incident-response plan for security threats. Federal and state regulators may require different responses to a breach. State laws are usually enforced by the state attorney general and typically deal with things like notification requirements in the event of a data breach. Federal laws apply to protection of personally identifiable information (PII). Failure to notify state regulators and consumers in accordance with state laws can amplify

Continued >>

All rights reserved. Third-party reproduction for redistribution is prohibited without contractual consent from Scotsman Guide Media.

<< Continued

enforcement actions, reputational risks and monetary damages.

The response plan should define what constitutes a breach. High-profile breaches with large volumes of PII are obvious, and many lenders use a loan-origination-system reporting database containing PII. What happens when it appears that the database may have been accessed by a hacker, but it is unclear by whom and whether information was extracted? Without monitoring technology, a lender has to assume the worst and presume all the information was compromised.

"Tone at the top" is an important third leg of an effective information-security program. Lending executives must embrace employee training, testing and monitoring to achieve appropriate levels of security. Originators, in particular, will look at the tone at the top to decide whether to take training and risk-reduction procedures seriously.

■ ■ ■

Information-security compromises are now a looming risk for mortgage lenders that must be addressed through executive-management engagement, ongoing governance activities and an appropriate risk-management plan that encompasses the entire organization. The core objective of managing information-security risk is to build a resilient system designed to identify, detect and respond to risks on a continuous basis across the organization.

The ability to meet this core objective is essential to minimizing business disruption as well as financial, regulatory and reputational losses. Most importantly, a significant improvement in a mortgage company's information security can be attained through training, careful use of technology and a proper tone at the top of the organization. ■

Reprinted from *Scotsman Guide* Residential Edition and **ScotsmanGuide.com**, August 2016

All rights reserved. Third-party reproduction for redistribution is prohibited without contractual consent from Scotsman Guide Media.