BY JEFFREY BERNSTEIN
Managing director of cybersecurity advisory services,
Marcum LLP

PREPARE TO FACE YOUR HACKER

You need a plan for when cybercriminals get inside

Commercial mortgage lending has become one of the prime targets for cybercriminals. Several large companies have fallen victim to cybersecurity breaches, data leaks, ransomware attacks and other compromising, exploitative actions.

Major breaches this past year at Capital One and First American Financial Corp. are the latest reminders that it only takes one gap in security for a hacker to create financial and reputational catastrophes. The bad news is that the threat is so pervasive that there is likely no way to entirely safeguard your business. If and when hackers do get inside your systems — and they likely will — you can take steps to lessen the damage they do. >>

ARTWORK BY KAREN STEICHEN

<< **Hacker** continued from Page 57

Some cybersecurity breaches are the result of targeted, organized crime. Many others start when trusted, authorized insiders accidentally open a malicious attachment or URL, visit an infected website or misconfigure a security control. Because of this, every person who has access to a lender's or mortgage broker's data can cause a security incident.

Regardless of how the hacker finds the way inside your systems, the consequences can be serious. A data breach can do immense damage to your brand and reputation. Your clients could be exposed to identity theft and fraud. In some states, your company also could face significant fines for failing to protect them. But what is it about loan originators that makes them targets of cybercriminals?

The simple answer is that mortgage companies have information that cybercriminals want. When commercial mortgage borrowers apply for a loan, originators often require a trove of personal information, including driver's licenses, social security numbers, tax returns, bank statements, W-2 forms, credit reports, employer information, family information, personal references and more.

Opportune targets

The pervasiveness of mobile computing, wireless networking, hosted cloud services and the internet of things also creates advantages for hackers, as they only need to find one vulnerable point to successfully perpetrate their attacks. Lenders and mortgage brokers often trade security for ease of use and access for their customers.

A mortgage company's "attack surface" makes it a fairly easy and accessible target. This refers to all of the end points where unauthorized users and attackers can enter or extract data. Furthermore, most mortgage companies market their products and services to the public. They typically assemble a warehouse of IP addresses, device ID profiles, e-mail addresses and other sensitive, identifying consumer information.

Typical mortgage transactions also involve the sharing of private data among multiple parties, including the borrower, the lender, title companies, insurers and appraisers, among many others. A financial institution's data is only as secure as its weakest business partner that has access to its data — a fact that was proven once again this past July with the massive breach at Capital One.

Capital One reported that the unauthorized individual was able to exploit a "configuration vulnerability" to steal records held in an Amazon Web Services database. The breach exposed an estimated 106 million credit-card applications from U.S. and Canadian citizens.

A single security deficiency also was identified as the culprit in an even larger breach uncovered this past May. First American, a Fortune 500 title-insurance company, exposed approximately 885 million sensitive records over several years. The leak was caused by an application-security flaw on its website. The hundreds of millions of digitized documents exposed were related to mortgage deals dating as far back as 2003 and included Social Security numbers, bank-account numbers and statements, and tax and mortgage records, among other private documents.

All of this sensitive data was openly accessible without the need to authenticate usernames or passwords. The data could be opened by anyone with an internet connection and web browser. To put the size of the First American breach into perspective, 885 million records is more than double the U.S. population. A simple application-security vulnerability assessment could have identified the deficiency and allowed the company to properly secure its data.

Definition

Incident response plan

A written plan with multiple distinct steps to assist information-technology professionals recognize and respond to cyberattacks, data breaches or other incidents involving digital technology. These plans may be tested annually, and specific employees may be trained and assigned to respond to incidents on a 24/7 basis.

Source: SecurityMetrics

The constant threat of a cyberattack, therefore, is real. But protecting the data is only one challenge. Financial-services companies also are likely to face tightened regulations. In reaction to numerous breaches over several years, the states of New York and California have already passed laws placing restrictions on how businesses handle a wide range of consumer data. The breaches at Capital One and First American, among many others, continue to shine light on the threat. More cybersecurity regulations for financial institutions are likely to follow.

It also is reasonable to assume that financial institutions will one day face much stiffer penalties for failing to protect consumer data. In Europe, heavy fines are already happening. Recent fines imposed by U.K. and European Union authorities include a $123 million fine against Marriott stemming from a 2014 consumer-data breach. In the U.S., privacy also is on the radar of the federal government. The Federal Trade Commission recently announced a $5 billion penalty to Facebook for privacy violations.

Damage control

Given the extent of the threat and the changing tactics of cybercriminals, financial institutions will likely never be able to stop breaches. Most lenders and mortgage brokerages are staffed by smart, highly technical, internet-savvy professionals. These organizations already have adopted effective enterprise security programs.

Companies regularly educate staff on security-awareness matters and the latest threats. They've implemented policies and procedures that govern how they can best secure their environments. They test for security vulnerabilities. They've adopted the latest cutting-edge technologies to secure their electronic infrastructure.

In short, these companies are doing almost everything right. But attackers continue to find ways to penetrate their defenses. One might ask, if large, well-equipped organizations like Amazon, Capital One and First American can't properly secure their systems and client data, how can others with less resources ever secure theirs?

The fact is that financial-services companies will never enjoy absolute security, but they can minimize the damage. They must use all available resources to prepare for the havoc that cybersecurity incidents can and will create.

Designing and implementing an incident response plan should be a top priority for any lender or mortgage broker. The plan will govern and direct how the organization will effectively identify and respond to the various day-to-day cybersecurity issues they might face. This plan defines what constitutes a breach and identifies key stakeholders, escalation procedures and other measures to be taken during an incident or event.

Lenders and brokerages need to be prepared to investigate cybersecurity compromises. A company can either hire an experienced cyber-response specialist or partner with an expert independent services provider. The bottom line is that an expert is needed to determine what has taken place, the source of the attack, the damage done, remediation tactics and next steps to avoid future occurrences.

■ ■ ■

For commercial mortgage lenders and brokers, falling victim to a cyberattack is not a matter of if, but a matter of when. Coupled with the growing challenges of government regulation, financial institutions are under more pressure today than ever to plan, protect and respond to cyberattacks. An incident response plan and data-forensics capabilities are now crucial tools for any lending organization's security. Proper response and compliance planning will protect a company over the long term. ■

Jeffrey Bernstein is managing director of cybersecurity advisory services for Marcum LLP. In his role, Bernstein advises clients in highly regulated industries on the protection of their networks, applications, systems, data, devices, people and property. Marcum LLP is based in New York City and is one of the largest independent public-accounting and advisory-services companies in the nation, with offices in major business markets throughout the U.S., Grand Cayman and China. Reach Bernstein at jeffrey.bernstein@marcumllp.com and follow him on Twitter @Jeff_Bernstein1.