SECONDARY MARKETING EXECUTIVE®

Reprinted with permission from the October 2015 issue

Cybercrimes And The Threat To Lender Data

How stronger security and response plans can protect lenders from a data breach.

By Lee Brodsky

It looks like 2015 will be one for the record books - but not in a good way. In its midyear data breach trends analysis report, Risk Based Security, a consultancy that helps firms with information security and compliance challenges, announced that 1,860 data breaches had been reported in the first six months of the year, breaking the midyear record set in 2014 by almost 200 cases.

With all of the media coverage surrounding cyber theft and the well-reported breaches of high-profile companies, it begs the question, why is this still happening? And, even more, what steps can a company, especially one in the mortgage industry, take to protect itself from a data breach?

No one is safe

The major data breaches that impacted large organizations including Sony, Target, Bank of America and, more recently, the IRS have been both a blessing and a bane for those advocating for stronger cybersecurity and response plans. On the one hand, these incidents have resulted in a stronger focus on data security, but they also caused many small and midsize companies to develop the misassumption that they're not big enough to warrant attention from cyber thieves.

That is an inherently flawed view, as it is on par with saying, "Let's not lock our front door because there are much nicer houses down the block." The truth is, mortgage banking firms are especially ripe for cyber attacks because their systems store the personal information of their customers and employees. What's more, data thieves know it is far more likely that a smaller company may not have good security measures in place.

Lee Brodsky

In this new age of cybercrime, attackers may not be setting out to target a specific company but, instead, are laying out traps across the Internet and through email (trojans, phishing attacks, worms, malware, etc.) to see who they can ensnare. If a worker on a lender's network clicks the wrong link, installs malicious software or is tricked into providing access information to the wrong site or people, the organization's whole network, including its customer and employee databases, could be compromised - and the attacker will have stumbled upon quite a treasure trove of valuable data.

Cybercrime is big business

Although movies and TV (and even some of the stories behind the recent Sony hack) might suggest hackers are looking to "hack the planet" and create anarchy, the truth is that hacking can be a profitable pursuit. The personal and financial info a hacker steals from a mortgage banking firm database is most likely enough information to create new financial accounts. That means they can open up new credit cards or checking accounts, running up debt and bad

checks using other people's names. Thieves can also use the stolen information to gain access to people's existing accounts and charge expenses to their credit cards or drain their bank accounts. In an even greater irony, the hackers can use the data obtained to take out home loans from other mortgage bankers.

Stolen data can be used to obtain driver's licenses or government-issued IDs, which the hackers can use to illicitly buy or lease vehicles, rent apartments, and obtain cell phone accounts. Social Security numbers can be used to gain employment for those in the country illegally, report income under another's name and gain access to government benefits, such as Social Security income or disability.

It is not likely that any one person or group is able to steal the data and commit all of these acts of fraud. However, like any growing industry, the cybercrime industry has developed a more complex supply chain. Hackers steal the data and sell that information down the chain to middlemen. Those brokers then find buyers who have the means and channels to further take advantage of the data and continue to make a profit.

Like any growing industry, the cybercrime industry has developed a more complex supply chain.

Another key moneymaking scheme involves the use of ransomware. Often by mimicking legitimate businesses and brands, cyber thieves convince the unwary to download software from an email or website that then encrypts the data on a user's hard drive or network. As the name suggests, the criminal then holds the data for ransom, demanding payment in exchange for releasing the files (although there's really no guarantee he will actually release the files upon receiving the money). In a similar vein, hackers can blackmail a person or company, threatening to release sensitive data if their demands are not met.

So, how much money can a cyber criminal make? Trustwave, a cybersecurity management firm, crunched some numbers in its 2015 Global Security Report. It estimates that a cyber criminal can run up about $5,900 in expenditures from just one ransomware-type scheme. That list of expenditures includes buying the ransomware software on the "underground market" so the thief doesn't need to know how to write code. Trustwave hypothesizes that a 30-day run of the exploit could net about $90,000. That's a 1,425% return on investment.

Like any moneymaking endeavor, the key takeaway here is cybercrime is built on profitability. The more and better the security measures a company puts in place, the more time-consuming it would be for a hacker to try and break through the system.

As in any business, time is money, so thieves are going after the low-hanging fruit: those with poor or no security in place.

The rising cost of a data breach

Each year, the Ponemon Institute, an organization that performs independent research on privacy, data protection and information security policy, conducts a data breach study. This year's study found that in 2014, U.S. companies spent an average of $217 per compromised record - a new record high.

The cost per record paid by companies in the financial services industry was even greater at $259. This is partially attributed to the fact that the financial services industry (which includes mortgage bankers) is more heavily regulated. In fact, under the Gramm-Leach Bliley Act (GLBA) or Financial Services Modernization Act of 1999, the U.S. Department of Justice has the authority to bring actions against breached financial institutions, leading to fines of up to $100,000 per violation.

To start to calculate the potential loss a lender could incur from a breach, one needs only to look at how many records are stored in a lender's database. A small database of 1,000 records could lead to a $217,000 loss. But, what if a lender has 10,000 or even 100,000 records? In fact, the study found that a data breach can cost a U.S. company an average of $6.53 million, an 11% increase from 2014.

Understandably, after a breach, higher-level managers are under greater scrutiny than in the past. It has been speculated that Target's CEO and chief information officer were both forced out after the company's data breach (though other poor business showings were most likely also a factor), and there was a strong, yet unsuccessful, effort to oust Target's board of directors. As part of the GLBA, the Department of Justice can go after a company's directors and officers, holding them personally liable for civil penalties of up to $10,000 for each violation. Directors and officers may also be targets of shareholder derivative lawsuits. So, it's not just a good business decision for company leaders to have the proper security and response systems in place - it may also be a good personal decision.

How to defend your company

The Ponemon Institute has determined that the most profitable data security investments that companies can make include developing an incident response plan, extensive use of encryption, business continuity management, the hiring or appointment of a qualified chief information security officer with enterprise-wide responsibility, employee training, board-level involvement, and insurance protection. Trustwave echoes this sentiment in its global report, which states that "recognizing a breach requires skilled people, well-defined processes and the right technologies."

Additional expenditures on the right team members or outside consultants and technology are a must. The Trustwave report also has some very simple, economical tweaks a company can enact to gain better protection. For instance, 28% of the 574 companies Trustwave studied can track their breach back to weak passwords, which was the top vulnerability exploited by hackers in the report. In fact, Trustwave notes that within these breached companies, the extremely hackable "Password1" was used 5,585 times. It was also the most common password used by companies in their study. So, at the very least, companies should develop stronger passwords, using a mix of lower case letters, upper case letters, numbers, non-alphanumeric characters and Unicode symbols.

> In 2014, U.S. companies spent an average of $217 per compromised record - a new record high.

Companies should also make their passwords longer. Trustwave estimates that an eight-character password can be cracked in a day using brute-force techniques with readily available technology. But, if a company were to increase its password length to 10 characters, it would take a hacker on average 591 days (19.5 months) to crack it. From a profitability perspective, there's no way that a 591-day hack is cost-effective for a cyber thief, and there's every reason to believe that creating a 10-character password is cost-effective for a business.

Cyber liability insurance

During the Mortgage Bankers Association's National Technology in Mortgage Banking Conference & Expo, former Homeland Security Secretary Tom Ridge said, "You have to assume you're going to have a breach. What is your approach? And you'd better have a response plan - and hope you never have to use it."

If a company must assume it is going to have a breach, it logically follows that it should protect itself with insurance specifically designed to provide coverage for the losses incurred by a breach. In fact, as mentioned previously, the Ponemon Institute recommended insurance as one of the most profitable investments a company can make to reduce the costs of a breach. If a hacker does find his way into a company's system, cyber liability insurance is often the last defense.

For this reason, cyber liability insurance is quickly becoming one of the most important and most requested coverages by mortgage banking insurance companies. This coverage often provides for the expenses associated with a data breach, including tech and legal fees, crisis management, public relations, and notification and credit monitoring subscriptions. A more extensive policy might also include business interruption coverage - which is crucial if a business has to shut down while the breach is resolved - and reimbursement for any regulatory fines or penalties.

It is important for mortgage lending businesses to realize their general liability insurance is going to provide little to no coverage for such a major data breach. Similarly, Fidelity and Mortgage Errors & Omissions, both of which are part of a Mortgage Bankers Bond and are required by investors, warehouse lenders and government-sponsored enterprises Fannie Mae and Freddie Mac, won't provide any protection. In fact, despite the all-consuming damage a data breach can cause, cyber liability insurance isn't required by any of these entities or any regulatory agencies. Yet, keeping in mind the $217,000 loss associated with a database of just 1,000 records or the fact that the average total loss incurred by breaches is $6.53 million, it might be the only thing keeping a company's lights on and doors open after a breach. SME

Lee Brodsky is president of the Mortgage Banking Insurance Group at JMB Insurance, where he specializes in operational insurance for the mortgage banking industry. He can be reached at lbrodsky@jmbins.com.