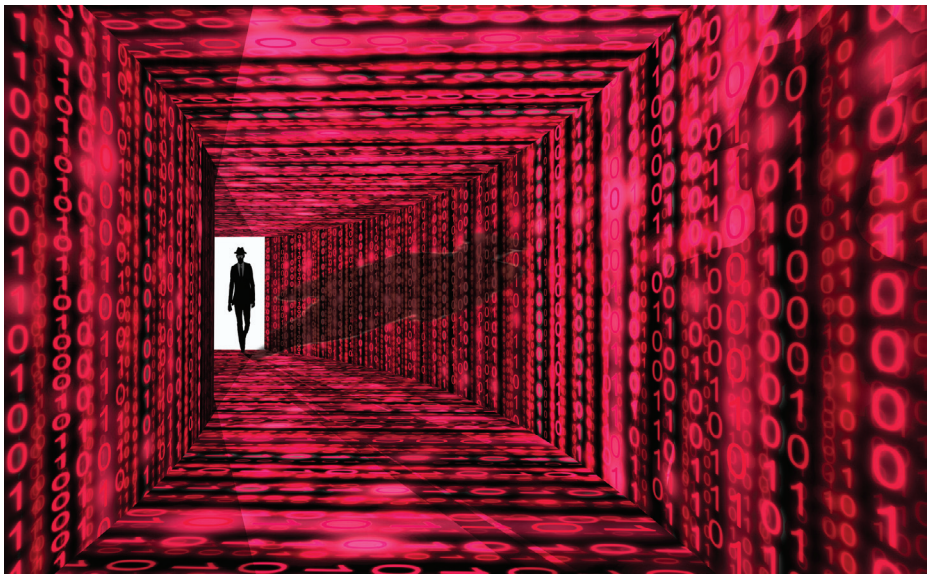
SECONDARY MARKETING EXECUTIVE®

Reprinted with permission from the November - December 2016 issue

Not A Matter Of If, But When ...

Now more than ever, mortgage lenders must protect their precious data from cyber attacks.

By Lee Brodsky



In the past few months, the news has reported on a record-breaking breach suffered by Yahoo, the barrage of hacked emails from members of the Democratic Party and a massive cyber attack that shut down a number of major online entities, including Twitter, Amazon, Netflix and PayPal. Although these attacks would seem to act as a warning sign that businesses need to better protect their data and their companies from the effects of a cyber attack, many executives instead dangerously assume they're safe. "After all," the reasoning goes, "hackers are only interested in huge targets, such as multinational corporations and political parties. They won't go after me. I'm too small."

Lee Brodsky

Of course, that outlook flies in the face of current statistics, which suggest that every company - no matter the size - is at risk. In its 2016 Internet Security Threat Report, Symantec noted there is plenty of hacking to go around. Of the companies in its study, small businesses (fewer than 250 employees) accounted for 43% of all attacks, midsize (250 to 2,500 employees) 22% and large corporations (2,500+) 35%. The report also noted that there has been a steady increase in attacks on companies with fewer than 250 employees over the last five years. In fact, attacks on those companies jumped 11% from 2014 to 2015.

One explanation for this jump in attacks on small to midsize companies is obvious. Hackers know these companies are less likely to have a data security plan in place, making them an easier target. Even more, it's becoming easier for them to initiate attacks through automated malicious code that gets access to your system and sends back the data. Thanks to these unmanned attacks, they don't need to expend much energy to attack smaller companies, making it more worth the effort.

Now, in addition to the fact that a company's data may not be well protected and hacking has become easier, throw into the mix that this company is in the mortgage banking business and collects personal information from its customers, prospects and employees. Put that all together, and it's no stretch of the imagination to see how a lender could be the perfect target for an enterprising cyber thief.

What do cyber thieves want?

Cyber thieves want data, and the data you collect is particularly valuable to them. In 2015, according to the Symantec report, the following top information exposed can all be categorized as personally identifiable information (PII):

1. Real names (exposed in 78% of all breaches in the study);
2. Home addresses (44%);
3. Birth dates (41%); and
4. Government ID numbers, such as social security numbers (38%).

This is a shift from previous years when financial information, such as credit cards, was the stolen data of choice, enabling hackers to ring up fraudulent purchases on someone

else's dime. But, credit card companies and users have become quicker to notice atypical purchases, limiting the usefulness of stolen credit card data to the individual hacker and the black market value if he or she should try to resell the data. As a result, financial info (which includes credit card details and other financial credentials) has dropped from No. 4 in 2014 to No. 6 on the above list.

On the other hand, PII offers cyber thieves greater flexibility. Forget stealing one person's credit card data. With PII, a cyber thief can open up countless credit cards in another person's name. That hacker can also obtain fraudulent government IDs, apply for loans, commit health insurance or Medicare fraud, file for fraudulent tax refunds, resell the data, and more.

In a January press release put out by the Identity Theft Resource Center (ITRC), which tracks breach information made publicly available, it noted that 2014 was the year of the credit card breach, citing 64.4 million debit/credit cards exposed due to breaches. In contrast, 2015 saw breaches expose only 800,000 debit/credit cards. That significant drop occurred because hackers were putting their energies into stealing over 164.4 million social security numbers. Appropriately enough, the ITRC dubbed 2015 the year of the social security number breach.

Of course, this PII (along with a host of other valuable information) is the exact info a lender needs from customers and prospects when it originates or services loans. What's more, a lender collects much of this same information from it own employees. This helps explain why, according to the ITRC release, the financial/banking/credit industry was ranked third in number of reported breaches (behind business/service at No. 1 and healthcare at No. 2). This marks the first time the financial services industry has cracked the top three.

Potential cost of a data breach

The most important factor in determining the cost of a data breach is not revenue, number of employees or even number of originated loans, but, rather, the total number of records in a lender's database, which can include past and present customers, prospects and employees.

In its 2016 Cost of Data Breach Study, The Ponemon Institute, an organization that conducts research on privacy, data protection and information security policy, found that the average cost per lost or stolen record for a U.S. company in 2015 was $221. It further broke down that $221 into $76 spent on direct costs incurred to resolve the data breach, such as investments in technologies or legal fees, and $145 spent on indirect costs, which included notification efforts and customer turnover.

Even more, the average cost per lost or stolen record for a company in the financial industry was $264. This rate was greater than the average because this industry is more highly regulated (companies could face fines for their breaches) and because, when breached, companies in this industry suffer a higher-than-average loss of business and customers.

So, using this average cost per record, even a database of only 1,000 records could end up costing you somewhere in the neighborhood of $264,000. How many records do you have in your database? Thousands? Tens of thousands? Hundreds of thousands? The Ponemon Institute found that, of the companies it studied, the average total cost of a data breach was over $7 million. What would the repercussions be if your company suddenly had to deal with a $7 million loss?

How can a lender protect itself?

The first step is to review current processes and inherent risks. Some of the main questions to ask include the following:

1. What data do you store?
2. Where is the data stored? What protections are in place?
3. Is it backed up? What protections are in place for the backups?
4. Who has access?
5. What devices are being used (computers, tablets, smartphones, printers, etc.)? Are they encrypted?
6. What are your agreements with third-party vendors?

The extent and cost of a data breach can be reduced if a lender puts into place data governance initiatives. These initiatives act as quality control protocols for how to protect, manage and use your data and should include appointing a chief information security officer, creating a business continuity management strategy that identifies the company's risk of a breach, developing an incident response plan and training employees on proper procedures, as well as making them aware of potential threats. Once the strategies are in place, a lender can then start looking at more tactical executions, such as installing data loss prevention software, which limits the ability of users to send sensitive information outside the corporate network, as well as encryption and endpoint security solutions, which ensure devices connected to your network follow a defined level of compliance and security standards.

Although the aforementioned recommendations will take some time to implement, there are other simpler solutions that you can begin undertaking right away.

Use strong passwords, password protocols

Passwords should be at least 10 characters and include a mix of lowercase and uppercase letters, numbers, and non-alphanumeric characters and symbols. Avoid using actual words because hackers can run software that checks for every word in the dictionary (and please, please, please don't use password, password1 or admin). One can also use a password generator (to develop a password) or aggregator (to store your passwords). Just make sure that if you're digitally saving passwords, the only way to access them is through a password that you must remember and key in - don't store that password on your computer or device. This way, you limit the damage if a computer or device is lost or stolen.

Lenders need to be smart in how

they use passwords. Don't reuse passwords in multiple places (otherwise, a compromise of one can give a hacker access to other systems). Instead of sharing one account and one password, give everyone unique login credentials. That way, management can easily shut down and create a new account if one is compromised. Additionally, it will be easy to turn off that account once an employee is no longer with the company (and it protects the business in case the employee doesn't leave on the best terms). Lastly, compartmentalize access. By giving employees access to only the data they need and not the whole system, one can limit exposure should a breach occur.

Update aggressively, back up regularly

Keep the software, browsers and applications on your computers, phones, etc., up to date. Old software can have vulnerabilities that hackers can exploit.

If data gets corrupted, gets locked up in a ransomware scheme or undergoes some other emergency, a lender should be able to restore the backup quickly to minimize downtime.

Educate your team

Many breaches occur because employees just aren't aware of the cyber threats, especially how thieves might try to deceive them through email, websites and now social media. Train them on how to protect their passwords and properly react to attachments, links and information requests sent to them in emails (by both trusted and unknown senders) and to let the proper team members know if they notice anything suspicious. Ultimately, encouraging awareness and good habits among the team can positively affect data security.

Good procedures will greatly limit the chance a lender has of suffering a data breach. But, human error, the speed with which new technologies are introduced and the tenacity of cyber thieves mean there's no 100% solution. So, should a breach actually occur, cyber liability insurance can be a second line of defense, protecting a company from the immense expenses that it might otherwise have to pay out of pocket.

The biggest threat

The biggest threat to a lender's business is inaction. A lender needs to acknowledge that a cyber attack against its business is a possibility; therefore, management must make a conscious decision to take action and protect company data, customers, its business and its bottom line.

Nonetheless, despite all of the warning signs, many lenders are still not motivated to act, letting the supposed cost, time and labor of enacting proper protocols or purchasing insurance outweigh the very real and much higher cost they'd incur if their systems were breached. Consider the following data from CFO Magazine's 2016 survey of 233 chief financial officers (CFOs):

- 22.0% reported an attack in the last 24 months;
- 57.5% said cybersecurity is a top concern;
- Only 23.9% are buying cyber insurance; and
- Only 11.7% have taken the time to estimate the cost of a cyber attack.

Given the number of past attacks and the respondents' concern about future attacks, it's actually startling to see how few CFOs in the survey are estimating the potential expense of an attack and how few are seeking out insurance.

Data breaches are a part of business now. Like property and casualty or workers' compensation, a lender needs to treat the cyber threat like any other risk to its business and purchase the appropriate coverage. However, it's true that a company may have to spend thousands or even tens of thousands now to enact a cyber plan that puts into place safe protocols and includes cyber liability insurance. Keep in mind that the average cost in 2015 for a data breach was more than $7 million. Investing now can potentially save your company millions in the future. SME

Lee Brodsky has specialized in insurance for the mortgage banking and financial services industry for more than 30 years. In May 2004, he established Mortgage Banking Insurance Group at JMB Insurance. He can be reached at lbrodsky@jmbins.com.