Your Client's Cybersecurity Threat Is Your Threat Too

BY MYRA THOMAS

The specter of cybercrime haunts every industry, but none more so than financial services. If there is considerable money involved or sensitive client data to steal, then there is certainly some cybercriminal looking for a financial firm to target. As secured lenders step up their efforts to secure their own systems and data, there is a growing understanding of the complexity of that task. Asset-based lenders and factors are increasingly aware that their cybersecurity procedures must be ongoing and dynamic to thwart a network intrusion and to quickly shut down and mitigate a hack if it does happen.

As lenders, the information from current clients and prospective clients is extremely sensitive. “We are looking at hundreds of prospects a year, so the amount of information we receive is staggering,” says Jennifer Palmer, CEO of Gerber Finance. “Safeguarding this information has to be one of our greatest priorities.” But secured lenders are also realizing that not only should their cybersecurity be top of mind, their clients’ cybersecurity procedures need to be as well.

Understanding the Relationship

Ultimately, a client’s cybersecurity measures do impact the asset-based lender and factor. Secured lenders receive a considerable amount of information from their potential and current clients, including detailed and historical financial data, proprietary information, background information on the management team, credit reports, and much, much more. That data needs to be protected, so it isn’t manipulated. Palmer notes, “At Gerber, we are concerned about the risk a hack to our client’s information would pose to our client and to us. We need to ensure safeguards are in place to protect our own data, as well as theirs, and all the more reason to have a conversation with our clients about the importance of protecting theirs.” That data, as any cybercriminal would know, is valuable on the dark Web, so it’s important for asset-based lenders and factors to not only secure their own systems and networks, but ensure that their clients are doing the same.

Whether it’s a cybercrime that leads to theft of the client’s data or a ransomware attack that causes an interruption in the client’s business, the secured lender is obviously on the proverbial hook too. A major financial risk to the client certainly becomes the secured lender’s problem. Consequently, says Michael Stanley, managing director at Rosenthal & Rosenthal, the underwriting process has to take cybersecurity into serious consideration. The initial field exam is the time to assess the cybersecurity measures of a prospective client.

It’s a smart move, says Stanley, given the very real and ever-growing threat of data theft or ransomware. He notes, “In this climate, we feel it’s imperative for our clients to have the appropriate systems and procedures in place to protect themselves and their businesses. Throughout our initial field exam and review of the company’s books and records, our examiners question prospects regarding their cybersecurity procedures and confirm their servers are backed up to third-party outside locations, protecting themselves in the event of a cyber-attack.” The process should also assess whether or not a current cybercrimes insurance policy is in place.

What to Fear

The very nature of the secured lender’s and client’s business relationship requires that they be continuously interconnected. Palmer notes that secured lenders have access to their clients’ systems and, in turn, manage collection of their receivables. When clients need money to operate their business, they provide their secured lender more information to request it, and the lender then sends funds to their bank accounts. “We are sending out millions of dollars every day, which leaves us

Roundtable Participants

KEATRON EVANS
KM Cyber Security

VINCE MANCUSO
IconiQ Finance

JENNIFER PALMER
Gerber Finance

BUDDY PITT
Network Support Co.

MICHAEL STANLEY
Rosenthal & Rosenthal

potentially exposed," she adds. But what is the risk?

According to Keatron Evans, president at KM Cyber Security, the "bad guys" aren't always trying to hack into a lender's network directly. They may be more likely to try to get to the end user or, in this case, the client. Once a cybercriminal gains access to the secured lender's network via the client, they will act as if they are the client. Evans says that a malicious attack sometimes results in a client's funds being erased, or the cybercriminal will pretend to be the client and ask for funds to be paid out to a bank account. Cybersecurity efforts can take into account everything from password protection to a multi-factor authentication system for releasing funds.

Not surprisingly, the number of cybercrimes and the dollars directly lost from theft or business interruption is steadily rising, particularly as businesses continue to digitize, the amount of financial transactions increase, and clients demand a more seamless and real-time relationship with their lenders. "Cybercrimes are happening more and more frequently, but the cybercriminals are usually very smart and keep the amounts under a certain threshold, so they don't get the U.S. Secret Service involved," Evans adds. But even a small financial theft from a client can result in a bigger problem, especially if the word gets out. Given the media's focus on cybercrimes, secured lenders need to be well aware of the reputational risk involved with the theft of a client's data or a client's own customer data.

Cybercriminals can also cause extreme business disruption... Stanley notes that secured lenders need to upgrade systems consistently, realizing that the process is always ongoing. Says Stanley, "We are constantly upgrading our firewalls and software protection systems. These hacks are becoming more and more complex, so cybersecurity is an important issue our company is focused on. At Rosenthal, we pride ourselves in the strength of our platform and how transparent we are with our clients."

Cybercriminals can also cause extreme business disruption, which may take considerable time and money to resolve. Stanley notes that secured lenders need to upgrade systems consistently, realizing that the process is always ongoing. Says Stanley, "We are constantly upgrading our firewalls and software protection systems. These hacks are becoming more and more complex, so cybersecurity is an important issue our company is focused on. At Rosenthal, we pride ourselves in the strength of our platform and how transparent we are with our clients. As a result, this opens us up to potential threats that we need to protect ourselves against."

How to Respond

That real-time connection and seamless relationship that secured lenders pride themselves on can also be an area of concern, if cybersecurity isn't considered. The threat could come from a cybercriminal finding a vulnerability in a network and introducing sophisticated malware, or it could be a relatively simple attack caused by an untrained and unsuspecting employee falling for a phishing attempt and clicking a hyperlink on an email and inviting a cybercriminal into the network. And, the damage caused from the phishing attack could be just as great as the more sophisticated hack.

Palmer points to a situation at Gerber Finance, when client email addresses were spoofed. "We've received loan requests to new suppliers and new bank accounts," she says. "In some cases, the requests for funds were as high as $500,000. Fortunately, we've always caught these attacks before any damage was done, but the negative impact could have been huge. Had our team not been extremely cautious and our safeguards not been in place, these situations could have been a disaster."

Obviously, those safeguards in place need to deal with not only systems and networks, but also with the secured lender's and client's employees, says Stanley. He adds, "We attempt to educate our employees and clients on potential threats and advise them to filter any suspicious items through our IT departments to be properly evaluated." However, just as secured lenders up their cybersecurity efforts, hackers get

more sophisticated.

Cyber analytics and user behavior analytics tools can prevent some of the risk, and that's where outside and expert cybersecurity advice can help. But no matter what the secured lender or client does, Evans notes that, at some point, there will be a breach. "What you want to do is to have the least amount of impact," Evans says. "Often, it's how quickly you detect it, respond, and contain it that can be even more important than the prevention." The question is whether the client will be able to recover from the cyberattack.

A strong business and financial continuity plan can often get a client through a cyberattack, says Buddy Pitt, director of client services at Network Support Co. "It all really comes down to the measures they're taking," he adds. "Someone will always be knocking on the door, constantly trying different types of attacks."

Simply put, most businesses don't have the right people to prevent and deal with the many types of cybersecurity breaches that could happen, says Pitt. It takes outside cybersecurity experts to audit IT before and after a breach. The secured lender and, especially, the client are unlikely to know the right questions to even ask. He notes that it takes professional cybersecurity advisors to do proper due diligence and audit the secured lender and client. "With the many data breaches, people are certainly getting numb to the risk," Pitt adds. But he notes that can be a costly mistake, since a loss of productivity and an inability to service clients, as well as the secured lender's and client's reputation, are all at stake.

A New Wrinkle to Consider

According to Vince Mancuso, president and CEO of IconiQ Finance, the entry of digital competitors into the secured lending community means cyberthreats are becoming ever more real for the industry. The risk can come from a third-party vendor who is providing technology for core business functions, he adds. "If you are a lender highly dependent on the automated exchange of information, you've often not built the platform yourself, so there are additional layers of risk." The cybercriminal could penetrate the lender via the third-party vendor who may have created the code for the lender or the client, so that the client can then send their data to the lender.

Given the dynamics, it's not enough for secured lenders to develop best practices and then sit on their laurels. "The industry is highly dependent on technology to keep the business thriving and adapting to change," says Mancuso. It's not enough to settle for today's security measures. "You have to ask how are you going to defeat attackers tomorrow." Some might assume that cyber insurance is one way to do just that.

According to Mancuso, no one can be an expert in all of the cyber risks out there. "I think cyber insurance, eventually, will be one of the most cost-effective ways to deal with the risk," he adds. However, the cyber insurance landscape is a bit complicated, at least for the moment. Mancuso notes that clients have a difficult time understanding exactly what type of cybercrimes the policies cover. Plus, there doesn't appear to be one consistent type of cyber insurance policy. He notes, "The policies really need to be dumbed down a bit for the client, so they can easily see what is reimbursable." Plus, cybercrime riders attached to other types of insurance, such as E&O policies, may not adequately cover all cybercrimes. He surmises that cyber insurance will become more common and standardized in the future, but that it will take secured lenders to get their clients to routinely consider buying it.

A Look Ahead

At the end of the day, the right policies and procedures, as well as the right people on the task, are just as important as the technology to prevent a cybercrime. One of the bigger mistakes that secured lenders might make is in assuming the larger the client, the better prepared they will be for a cyber threat. According to Palmer, business leaders could theorize that a bigger company would have "greater systems and technology to help minimize the threats." She adds, "We have seen many small companies with better systems in place than larger ones to help protect against these threats." It takes people and technology working in tandem to constantly monitor, prevent and mitigate a cybercrime.

Cybercriminals are constantly looking for vulnerabilities in systems and networks and, if the secured lender isn't the target, then the client just may be. Outside advice and cybersecurity expertise is certainly important, given the amount of threats financial firms face. Palmer adds, "First, you need to spend money on getting the right advice, second, on purchasing the right technology and, third, you need to spend the time and dedication in implementation, maintenance, evaluation and upgrades." Certainly, secured lenders can't be expected to be technological wizards. It takes leadership to make cybersecurity a priority in the organization, and to demand the same of the client, to make a lasting impact.

Myra Thomas is an award-winning editor and journalist with 20 years' experience covering the banking and finance sector.

MYRA THOMAS