DARK WEB

THE STYLISTICS ONCE SANG THAT "PEOPLE MAKE THE WORLD GO 'ROUND." THAT MAY WELL BE TRUE, BUT WHEN IT COMES TO CYBERSECURITY, IT'S ALSO PEOPLE WHO CAN CAUSE YOUR COMMUNITY INSTITUTION A WORLD OF HURT. IN FACT, THE BIGGEST THREAT FACING YOUR INSTITUTION MAY BE AN INTERNAL ONE.

Reprinted with permission

When most people think about cybersecurity breaches, there's a tendency to focus on the big splashes – the major customer data heist at a national retailer or the global ransomware attack that threatens to shut down businesses of all shapes and sizes. Yet while community institutions certainly need to keep their guard up against these types of large-scale, high-profile assaults, the real threat to their day-to-day business likely lies in a far more pedestrian, run-of-the-mill scenario that might play out something like this:

Jim in accounting clicked on a bad link in an email.

It's not exactly the kind of riveting, torn-from-the-headlines type of incident that screams out for a Movie of the Week, but the truth is that this kind of boring everyday miscue is, without question, the most likely way in which a community institution is going to become a victim of a cyberattack. According to a 2017 data breach investigations report by Verizon, 43% of hacks employ social engineering tactics to prey on unsuspecting or error-prone employees. When successful, those breaches can range in cost from significant to devastating for a community institution, incorporating not only direct monetary losses, but litigation costs, remediation expenses and reputational damage as well.

THE PEOPLE PROBLEM

"The biggest threats today come down to people," says Jay Schulman, a principal at RSM US LLP, and a leader in the firm's

> Having timely responses, and the right responses, is such an important piece of this preparation. Your reputation is probably going to take a hit, so how you respond to that and deal with that is crucial.
>
> Mark Boettcher, Senior Manager – Risk Advisory Services, Baker Tilly Virchow Krause

privacy and security practice. "If you think about all of the technology and great software that companies can buy to protect themselves, ultimately they're still at the mercy of someone clicking on a bad link or falling into a reply-and-response wire fraud transaction. It still comes back to the simple fact of people making mistakes."

Indeed, while smaller institutions have stretched their budgets in order to invest tens of thousands of dollars in security solutions to keep their data and systems safe, their biggest vulnerability continues to reside within. Jeff Olejnik has seen the impressive technical investments that many institutions have made in the name of cybersecurity, and he believes their defenses tend to be more advanced than those at most non-financial organizations. Nevertheless, when it comes to assessing where their softest spots remain, the director in the risk advisory services area at Wipfli LLP certainly shares Schulman's view.

"People are the weakest link," Olejnik says. "Even with the more sophisticated technical controls, a mistake made by an individual who clicks on a link they shouldn't, moves confidential information to a USB device or leaves an unencrypted laptop in a car that is stolen can lead to big problems."

STEPS TOWARD SAFETY

Given the likelihood that employees are going to be the conduit through which a potentially damaging cyberattack penetrates an institution, it stands to reason that one page in the handbook or an introductory training video that may have once constituted the entire cybersecurity program probably won't suffice in the current environment. Mark Boettcher, a senior manager of risk advisory services at Baker Tilly Vichow Krause says institutions need to make sure their assessment and mitigation programs have kept pace with the changing nature of the threats.

"A risk assessment is essential, where you really look at what vulnerabilities you have within your IT environment and what procedures you have in place to address those areas," he explains. "On an ongoing basis, institutions should be doing vulnerability scanning and penetration testing on the network."

Olejnik notes that in addition to the kind of vulnerability assessment that Boettcher describes, smaller institutions should also have a particular mindset when it comes to cybersecurity.

"There's no silver bullet and 100% protection is not possible," he says.

Reprinted with permission

THE 20/80 RULE

Jay Schulman wants to be 100% frank – community institutions simply cannot do 100% of the things that need to get done to ensure their system security. While the banking behemoths of the world may be able to spend upwards of $500 million a year on cybersecurity, community institutions (who might have less than that outlay in total assets) should use their more limited resources to instead shoot for the 20/80 rule, or, as he explains it:

"What 20% of things can you do to have an 80% impact on security?"

Here are five things that Schulman says community institutions can do on a limited budget to get meaningful security coverage, regulatory appeasement and peace of mind.

KNOW WHAT'S ON YOUR NETWORK

Schulman knows it seems odd that an institution wouldn't know what's out there, but he says it happens more often than most people would think. Whether it's something a contractor plugged in or something an employee added years ago and forgot about, the first step in securing your network is to know what you're dealing with. "People forget about this step – they jump right into scrambling around to secure things," Schulman says. "But if you don't know what you have on your network, it's really hard to do anything else."

CONFIGURE WHAT'S ON YOUR NETWORK

When Schulman talks about this step in the context of the 20/80 rule for community institutions, he stresses that you're just looking for basic protocols, such as how often you're asking people to reset passwords or how many times they can attempt login before they're frozen out – not necessarily the lockdown versions one might find at Chase or U.S. Bank. "It's just a matter of making sure you've thought through all of these basic things and taken steps to make them uniform across your entire environment," he says. "It doesn't have to necessarily be the best, but uniformity is the key."

PATCH WHAT'S ON YOUR NETWORK

Schulman goes back to the WannaCry ransomware attack from earlier this year, noting that a patch that had come out a few weeks before could have protected those victims. "Patching on a regular basis – which can in and of itself be a challenge – will really go a long way toward keeping you protected," he says.

PROTECT YOUR ADMINISTRATIVE ACCOUNTS

This step actually involves two avenues – IT people using administrator accounts and non-IT employees with administrative rights on their machines. In the case of the former situation, which is quite common, the concern is that any bad link or email that IT person might click on by accident puts the entire institution at risk, giving a hacker access to the whole organization. In the latter scenario, Schulman says institutions need to take control of those administrative rights. "Turning off that access so that employees can't install their own updates is a wildly impactful move, since 85% of the malware that gets sent doesn't work on machines that don't have administrative rights," he explains. "Locking down these rights can be incredibly controversial around the office, but it's also a major step toward being more secure."

TRAIN YOUR EMPLOYEES

Cybersecurity isn't just about money – knowledge is power when it comes to heading off the most common breaches. "This is clearly an essential piece," Schulman says, "since most attacks originate with an employee clicking on a bad link or opening a bad email."

TOO SMALL TO NAIL?

Are community institutions – with their lower profiles and lower asset levels – less likely to draw the unwanted attention of a hacker than the big banks? Don't count on it, says Jay Schulman.

"A lot of community institutions haven't thought about all of the ways that these attacks might reach them and aren't necessarily experienced with them. So while attackers might find more efficiency at the big banks, they may find a community institution that isn't quite as prepared to fend off their advances. In this case, going after the smaller, softer target of the community institution could be to their advantage.

"This is where what we call 'threat intelligence' comes into play. Institutions need to start thinking about all of the different ways someone might attack them or their customers and, more importantly, how they're going to respond when it happens. A lot of what we see today are generic, 'drive-by' types of attacks, but you have to start to think about how you're going to respond if somebody decides to very specifically target your institution."

"But one thing that small institutions should do is take a layered approach to security assessment and testing. The IT audit or perimeter vulnerability assessment that is done each year is great, but it may give a false sense of security. Penetration testing, red-team exercises, social engineering and disaster recovery testing should be integrated into the overall threat mitigation and assessment routine."

A good cybersecurity plan should not be limited to protection only, however, but should also include the institution's outline for how it will respond when an attack occurs. Both Olejnik and Boettcher caution that a plan that fails to address resiliency, continuity and decision-making in the wake of a breach is not where it needs to be, regardless of how strong one's external defenses appear to be.

"For banks and credit unions, it's not a matter of if they get hacked, it's really just a matter of when," Boettcher says. "For this reason, I think the resiliency part is almost more important than the prevention side. It's critical for an organization to have a plan for how it would handle a breach and what it would do to resume operations. For example, what is the institution going to do if it gets hit by ransomware? Has leadership thought through whether they're going to pay the ransom, or are they going to have procedures in place that allow them to continue to operate without access to those IT systems? This is also important just from a general crisis management standpoint – from contacting customers to dealing with the media and things like that. Having timely responses, and the right responses, is such an important piece of this preparation. Your reputation is probably going to take a hit, so how you respond to that and deal with that is crucial."

BUILDING A CULTURE OF SECURITY

Of course, the most important piece of any institution's cybersecurity preparedness comes back to the people problem, and how employees are trained to recognize and respond to the insidious threats that are certain to come their way. The goal should be to get to a place where everyone in the institution – from teller to manager – understands that security is an all-hands-on-deck kind of proposition. Anyone can be a target, so everyone needs to be on guard.

"Making sure employees are trained and are constantly thinking about whether the emails they get are legitimate can be a real challenge," Schulman says. "I think a lot of community institutions use some great technology outsourcing partners or they may have some great in-house technology, but ultimately if their employees are clicking on bad things or replying to malicious emails, it's really going to hurt them. It's a challenge for every industry, but when you have limited resources to make sure that kind of persistent training happens, it really puts your company at a significant disadvantage."

Schulman says there are a number of ways for community institutions to approach employee training, from expensive self-configured software programs that force employees to undergo training the minute they click on a malicious test email (thus immediately tying their behavior to the instruction) to the cheaper (and less effective) route of refresher sessions that still use real-world examples to help get the point across. Whatever method an institution ultimately chooses, the ideal outcome is a board and management team that sees the human element of cybersecurity as just as important as the technical side, and a staff that is vigilant and aware at all times.

"It starts with the tone at the top," Olejnik believes. "Building a culture of cybersecurity awareness cannot be done with just a once-a-year training session or having employees read a policy. A good training and awareness program will include a variety of elements including formal training, regular awareness touch points, testing and measurement. Most importantly, executives need to communicate their support for this type of effort and back it up with ongoing education and awareness campaigns." ▪

forward, a publication of the Financial Managers Society
Published for:
Financial Managers Society, Inc.
1 North LaSalle Street | Suite 3100 | Chicago, IL 60602-4003
FMSinc.org | 800-ASK-4FMS
Copyright© 2017, Financial Managers Society, Inc. All rights reserved.

Reprinted with permission

THE HIT LIST

The variety of cyberattack variations seems to grow and evolve almost by the week, but our three experts tend to see the following areas as the most likely to affect community banks and credit unions.

PHISHING > WIRE FRAUD

An oldie but a goodie, the classic email phishing scam designed to perpetrate a fraudulent wire transfer is often the least technical attack to prepare against – but just as often the most effective.

"Phishing has gotten much more sophisticated and hackers are getting a little smarter about their approach, so community institutions probably need to think outside the box a little bit in terms of being prepared to ward off these threats," Boettcher says. "At this point, they probably need to be thinking about new ways to test their defenses and procedures instead of doing the same kind of training and testing they've been doing for a while, because the threat has advanced since those tests were first put into place. Complacency is probably one of the biggest risks, so it's important to constantly look at different scenarios and plan for a more sophisticated threat."

MALWARE

Whether designed to steal an institution's customer information, shut down a key piece of its system or extort a ransom payment for access to its data, malware is a persistent and many-faceted threat that can arrive via malicious email, an unpatched machine or one of a dozen other avenues.

"Security in this area needs to be operationalized – it is not a once-a-year activity," Olejnik says. "Computers need to be patched and updated on a regular basis, passwords need to be changed, data needs to be backed-up and tested, and networks should be scanned routinely for vulnerabilities."

THIRD-PARTY RISK

As more and more key data-intensive services and functions are outsourced, institutions need to make sure they have a good vendor management program in place to help assess and monitor the risks introduced by new services and providers.

"It's important to make sure you understand where your data is and who has access to it," Boettcher says. "You need to make sure you're on top of your vendors and you understand what they're doing."

> "Computers need to patched and updated on a regular basis, passwords need to be changed, data needs to be backed-up and tested, and networks should be scanned routinely for vulnerabilities."
>
> Jeff Olejnik, Director – Risk Advisory Services, Wipfli LLP

ATLANTIC CAPITAL STRATEGIES, INC.

INVESTMENT ADVISORY SERVICES

Atlantic Capital Strategies, Inc. is an SEC-registered investment advisory firm located in Bedford, Massachusetts. Our senior bankers provide investment advisory services to community-based financial institutions, including commercial banks, savings banks and credit unions.

COMPREHENSIVE ADVISORY

- Tailored investment plan
- Security selection and best execution
- Pre-purchase analysis and ongoing monitoring
- Policy development
- Full regulatory reporting

INVESTMENT CONSULTING

- Annual portfolio reviews
- Credit monitoring surveillance
- Watch list reporting
- Market pricing
- OTTI analysis and impairment opinions

CONTACT: **Robert B. Segal, CFA,** *President & CEO* • 781-276-4966
bob@atlanticcapitalstrategies.com

WWW.ATLANTICCAPITALSTRATEGIES.COM

TOO SMALL TO NAIL?

Are community institutions – with their lower profiles and lower asset levels – less likely to draw the unwanted attention of a hacker than the big banks? Don't count on it, says Jay Schulman.

"A lot of community institutions haven't thought about all of the ways that these attacks might reach them and aren't necessarily experienced with them. So while attackers might find more efficiency at the big banks, they may find a community institution that isn't quite as prepared to fend off their advances. In this case, going after the smaller, softer target of the community institution could be to their advantage.

"This is where what we call 'threat intelligence' comes into play. Institutions need to start thinking about all of the different ways someone might attack them or their customers and, more importantly, how they're going to respond when it happens. A lot of what we see today are generic, 'drive-by' types of attacks, but you have to start to think about how you're going to respond if somebody decides to very specifically target your institution."

"But one thing that small institutions should do is take a layered approach to security assessment and testing. The IT audit or perimeter vulnerability assessment that is done each year is great, but it may give a false sense of security. Penetration testing, red-team exercises, social engineering and disaster recovery testing should be integrated into the overall threat mitigation and assessment routine."

A good cybersecurity plan should not be limited to protection only, however, but should also include the institution's outline for how it will respond when an attack occurs. Both Olejnik and Boettcher caution that a plan that fails to address resiliency, continuity and decision-making in the wake of a breach is not where it needs to be, regardless of how strong one's external defenses appear to be.

"For banks and credit unions, it's not a matter of if they get hacked, it's really just a matter of when," Boettcher says. "For this reason, I think the resiliency part is almost more important than the prevention side. It's critical for an organization to have a plan for how it would handle a breach and what it would do to resume operations. For example, what is the institution going to do if it gets hit by ransomware? Has leadership thought through whether they're going to pay the ransom, or are they going to have procedures in place that allow them to continue to operate without access to those IT systems? This is also important just from a general crisis management standpoint – from contacting customers to dealing with the media and things like that. Having timely responses, and the right responses, is such an important piece of this preparation. Your reputation is probably going to take a hit, so how you respond to that and deal with that is crucial."

BUILDING A CULTURE OF SECURITY

Of course, the most important piece of any institution's cybersecurity preparedness comes back to the people problem, and how employees are trained to recognize and respond to the insidious threats that are certain to come their way. The goal should be to get to a place where everyone in the institution – from teller to manager – understands that security is an all-hands-on-deck kind of proposition. Anyone can be a target, so everyone needs to be on guard.

"Making sure employees are trained and are constantly thinking about whether the emails they get are legitimate can be a real challenge," Schulman says. "I think a lot of community institutions use some great technology outsourcing partners or they may have some great in-house technology, but ultimately if their employees are clicking on bad things or replying to malicious emails, it's really going to hurt them. It's a challenge for every industry, but when you have limited resources to make sure that kind of persistent training happens, it really puts your company at a significant disadvantage."

Schulman says there are a number of ways for community institutions to approach employee training, from expensive self-configured software programs that force employees to undergo training the minute they click on a malicious test email (thus immediately tying their behavior to the instruction) to the cheaper (and less effective) route of refresher sessions that still use real-world examples to help get the point across. Whatever method an institution ultimately chooses, the ideal outcome is a board and management team that sees the human element of cybersecurity as just as important as the technical side, and a staff that is vigilant and aware at all times.

"It starts with the tone at the top," Olejnik believes. "Building a culture of cybersecurity awareness cannot be done with just a once-a-year training session or having employees read a policy. A good training and awareness program will include a variety of elements including formal training, regular awareness touch points, testing and measurement. Most importantly, executives need to communicate their support for this type of effort and back it up with ongoing education and awareness campaigns." ▪

forward, a publication of the Financial Managers Society
Published for:
Financial Managers Society, Inc.
1 North LaSalle Street | Suite 3100 | Chicago, IL 60602-4003
FMSinc.org | 800-ASK-4FMS
Copyright© 2017, Financial Managers Society, Inc. All rights reserved.

Reprinted with permission

THE HIT LIST

The variety of cyberattack variations seems to grow and evolve almost by the week, but our three experts tend to see the following areas as the most likely to affect community banks and credit unions.

PHISHING > WIRE FRAUD

An oldie but a goodie, the classic email phishing scam designed to perpetrate a fraudulent wire transfer is often the least technical attack to prepare against – but just as often the most effective.

"Phishing has gotten much more sophisticated and hackers are getting a little smarter about their approach, so community institutions probably need to think outside the box a little bit in terms of being prepared to ward off these threats," Boettcher says. "At this point, they probably need to be thinking about new ways to test their defenses and procedures instead of doing the same kind of training and testing they've been doing for a while, because the threat has advanced since those tests were first put into place. Complacency is probably one of the biggest risks, so it's important to constantly look at different scenarios and plan for a more sophisticated threat."

MALWARE

Whether designed to steal an institution's customer information, shut down a key piece of its system or extort a ransom payment for access to its data, malware is a persistent and many-faceted threat that can arrive via malicious email, an unpatched machine or one of a dozen other avenues.

"Security in this area needs to be operationalized – it is not a once-a-year activity," Olejnik says. "Computers need to be patched and updated on a regular basis, passwords need to be changed, data needs to be backed-up and tested, and networks should be scanned routinely for vulnerabilities."

THIRD-PARTY RISK

As more and more key data-intensive services and functions are outsourced, institutions need to make sure they have a good vendor management program in place to help assess and monitor the risks introduced by new services and providers.

"It's important to make sure you understand where your data is and who has access to it," Boettcher says. "You need to make sure you're on top of your vendors and you understand what they're doing."

> "Computers need to patched and updated on a regular basis, passwords need to be changed, data needs to be backed-up and tested, and networks should be scanned routinely for vulnerabilities."
>
> Jeff Olejnik, Director – Risk Advisory Services, Wipfli LLP

ATLANTIC CAPITAL STRATEGIES, INC.

INVESTMENT ADVISORY SERVICES

Atlantic Capital Strategies, Inc. is an SEC-registered investment advisory firm located in Bedford, Massachusetts. Our senior bankers provide investment advisory services to community-based financial institutions, including commercial banks, savings banks and credit unions.

COMPREHENSIVE ADVISORY

- Tailored investment plan
- Security selection and best execution
- Pre-purchase analysis and ongoing monitoring
- Policy development
- Full regulatory reporting

INVESTMENT CONSULTING

- Annual portfolio reviews
- Credit monitoring surveillance
- Watch list reporting
- Market pricing
- OTTI analysis and impairment opinions

CONTACT: **Robert B. Segal, CFA,** *President & CEO* • 781-276-4966
bob@atlanticcapitalstrategies.com

WWW.ATLANTICCAPITALSTRATEGIES.COM