Credit Union MAGAZINE
Credit Union National Association

MARCH 2019

Cybersecurity safeguards

Increasing threats need a range of protective measures.

TED GOLDWYN

In November 2018, Marriott International announced a major data breach affecting up to 500 million guests of its Starwood Hotels subsidiary.

The perpetrators stole an unusually rich treasure trove of personal information including names, phone numbers, email addresses, passport numbers, dates of birth, and departure information.

This event represented one of the largest data breaches in years. In 2018, 446.5 million records were exposed in more than 1,100 breaches across a range of industries, according to the Identity Theft Resource Center.

Last year, financial institutions experienced 122 breaches affecting 1.7 million records through Nov. 30, the center reports. Most significant among these was a reported breach at SunTrust Bank, which affected up to 1.5 million customer records, *USA Today* reports.

As bad actors become bolder and more sophisticated, credit unions must stay abreast of preventive measures to protect members and employees from the risk of cybersecurity attacks.

A looming threat

Cybersecurity experts are keeping a close watch on several emerging threats.

"People and passwords typically

Focus

- **People and passwords** typically constitute the biggest cybersecurity risks.
- **Regular employee training** is the best defense against cybersecurity attacks.
- **Board focus:** As threats become more sophisticated, credit unions must take preventive measures to protect members and employees.

> AS COMPUTING POWER INCREASES, THE TIME IT TAKES TO CRACK A PASSWORD DECREASES.
>
> KEVIN IVY

constitute the biggest cybersecurity risks," says Kevin Ivy, security solutions engineer at TraceSecurity, a CUNA Strategic Services alliance provider of cloud-based information technology governance, risk, and compliance management solutions.

Credit union employees are particularly vulnerable to email and social engineering attacks, including phishing emails, ransomware, and spoofing, Ivy says.

"Many data breaches are password-related, where someone clicks on a faulty link in an email spoofed to look like it's from another employee or a member they know," he says. "They click on the link, financial information is transferred to the wrong person, and it's all downhill from there."

"The threat actors are evolving," says Peter Misurek, senior information security engineer at $2.4 billion asset Royal Credit Union in Eau Claire, Wis. "They're figuring out ways to circumvent protections. As with any organization, our weakest link is our team members because of the human element."

Misurek is seeing an evolution in email-borne threats. These include everything from "executables," or programs like Microsoft Word that are launched on a PC, to more sophisticated techniques designed to penetrate the latest antivirus and anti-spam software.

"With the rise of antivirus and other forms of prevention, many malicious payloads were being blocked, and weren't successfully delivered to the endpoint," Misurek says. "So, threat actors have evolved to the point where instead of delivering the executables via email, they try to deliver via a URL or a hyperlink within the email."

Cybercriminals amplify the effectiveness of these threats through social engineering, using a compromised mailbox of someone the target may have corresponded with. They include some contextual content around the hyperlink to make the email seem legitimate.

Fraudsters also use macros within programs like Microsoft Word and Excel to deliver malware, and even include malware in PDF attachments to try to circumvent the next generation of artificial intelligence-enabled email gateways and spam blockers, Misurek says.

"A lot of email gateways are starting to block social engineering attempts by reading the context of the emails," he says. "So now the bad actors are sending a very short email, but the actual social engineering text and malicious hyperlinks are included in the attached PDF."

Who are the bad actors?

Nation-states often are behind large-scale attacks against major international corporations like Marriott. Some countries can afford to expend significant resources over the course of years to infiltrate sophisticated databases.

Their goals typically are to gather corporate secrets, intelligence, or information they can use to monitor the movements of certain targets through international points of entry. Several news outlets have reported that Chinese state hackers were behind the Starwood breach.

Nation-states also have attacked financial institutions.

"Some nation-state actors are attempting to gain access to payment networks, such as SWIFT," Misurek says. "The end game is to move mass quantities of money in and out of financial institutions."

For smaller organizations like credit unions, however, perpetrators are more likely to be small-scale cybercriminals aiming to steal money.

"Credit unions in general are not targeted by the nation-state actors, but are threatened by smaller-scale actors," Misurek says. "Some credit unions have been hit by some pretty significant ransomware outbreaks. Their level of preparedness dictates how much these attacks affected them."

An ounce of prevention

Preventing data breaches and network intrusions requires implementing a range of measures including:

›Strong passwords. As technology improves, it's much easier for fraudsters to decode passwords quickly, allowing unfettered access to sensitive data and systems.

"As computing power increases, the time it takes to crack a password decreases," Ivy says. "Back in the day, it would take someone a long time to crack a simple password like 'password123.' Now, that could probably be cracked in less than five seconds."

For that reason, credit unions should implement strong password policies that require employees to use complex passwords and change them regularly.

"The risks are increasing because technology keeps improving," Ivy says. "We're so used to recycling our passwords every 90 days, where people fall into a pattern of adding a single character or the season to their existing password.

"While authentication techniques have improved over time," he says, "the implementation rate isn't there

yet for credit unions. That leaves them susceptible to data leakage or breaches via password attacks."

›Multifactor authentication. In addition to enabling strong passwords, multifactor authentication, which requires a user to provide verification via another device, is an established method of ensuring that a hacker does not compromise employee credentials.

"Multifactor authentication is a great way to prevent easy password hacks," says Ivy. "For example, when I log into most of my websites, I also have to open an app on my phone that gives me a one-time code that I enter after that password. That thwarts the chance of passwords being cracked."

›Clean-desk policies. Social engineering attacks aren't limited to the external realm. Fraudsters may try to infiltrate a credit union's physical facilities, as well. If staff don't secure sensitive information, a serious breach may result.

"Credit union employees often leave files of sensitive information on their desks when they leave for the day," says Ivy. "That's a bad practice. It takes just one person with malicious intent to grab a stack of loan applications and cause a data breach.

"Typically, we'll include a clean-desk policy review as part of our onsite engagements," he continues. "Most credit unions have a clean-desk policy that states if you're leaving your desk unattended for a certain period of time, you must put files in a locked cabinet out of plain sight."

›Mobile device management. As smartphones equipped with cameras, internet access, and social media apps become more prevalent in the workplace, employers are rightfully concerned about employees inadvertently capturing and sharing proprietary data via photos, emails, or other means.

A mobile device management solution can prevent or limit damage from such breaches, Ivy says, citing solutions such as AirWatch. "You can enroll an employee's device in a mobile device management platform, and if anything were to occur, you could lock the device or wipe it clean."

He also recommends creating an employee mobile device management policy that explains and reinforces the risks of employees mixing business and personal use on their devices.

›Encryption. Human error causes many cybersecurity attacks. But it's also important to protect data digitally. Paramount in this realm is encrypting your data, whether it's at rest, in transit, or backed up.

Some credit unions will encrypt data on the core processor and when it's in transit from the server to the employees' workstation—but not encrypt data on the nightly backup tape, Ivy says.

"We can't forget that data, in all forms and stages, should be encrypted," he says. "In addition to the human social engineering, encryption will stop people from being able to manipulate or read data at any point."

›Limiting traffic and access. With a membership largely defined by common attributes, such as geographic region or employer, credit unions are in a unique position to prevent intrusions. Royal Credit Union's membership primarily is located in Wisconsin and Minnesota, which allows its information security team to closely monitor website traffic and limit access from internet protocol

TOP FIVE CYBERTHREATS FOR 2019

1 Ransomware
Fraudsters typically send this through an email attachment that, once opened, downloads itself and starts corrupting data. Educate staff about the type of emails that typically contain such viruses and ask them not to download attachments from unknown sources.

2 Phishing
These targeted email attacks often work because they seem authentic and genuine. Ask employees not to share sensitive information with outside parties, and implement effective firewall and spam filters.

3 Data loss
This often is due to employees' use of personal devices. Implement a BYOD (bring your own device) policy, and secure the endpoints of the devices staff use.

4 Communication
Implement a clear strategy to prevent hackers from breaching your security measures.

5 Inside vulnerability
Effective endpoint management can protect the corporate network when accessed via remote devices.

Source: KnowledgeNile's 2018 Cyberthreat Defense Report

Cybersecurity

addresses that may represent malicious activity.

"We know there are neighborhoods on the internet that are riddled with crime, fraud, and malicious activity," says Misurek. "Because our membership is primarily based in the Midwest, we can limit traffic to our external presence, or traffic from our internal networks to our external presence, from high online fraud areas like Russia, North Korea, and China.

"We block a lot of that activity before it even becomes an issue for our networks," he adds.

Misurek also watches for certain suspicious patterns, such as use of the Tor network, which allows users to browse the internet anonymously.

"If someone walked into a branch wearing a hooded sweatshirt with the hood up and a ski mask over their face, we would quickly escort them out of the branch and call the authorities," Misurek says. "So why would we allow people to talk to our online banking platform or our public websites using an anonymizer proxy like Tor?

"We've gotten to the point of blocking those anonymizing networks," he continues. "That's an easy win for a credit union that doesn't have to deal with a global membership that larger financial institutions may have to deal with."

Training and education

The single most important step a credit union can take to prevent cybersecurity attacks may be regular, consistent, and thorough training and education.

"Training can't be simply a 'one and done' thing," says Misurek. "It has to be continual.

"Humans are notorious for changing their habits at one point,' he continues. "But when they experience stress within their lives they may act and respond in a totally different manner than they did previously."

Experts agree the human element is the most critical among a dynamic and increasingly dangerous world of cybersecurity risks.

Credit unions must remain vigilant, and equip their employees with the knowledge and tools to protect the cooperative and members who are entrusting their most sensitive data.

"Have your employees attend security awareness training on a regular basis," Ivy says. "Ensure that new staff go through the same training within 30 days of hire to ensure there are no vulnerable entry points into your facility or data."

Resources

- CUNA:
  1. CUNA Cybersecurity Conference with NASCUS: *cuna.org/cyber*
  2. Environmental Scan resources: *cuna.org/escan*
- CUNA Technology Council Security Summit: *cunacouncils.org*
- Identity Theft Resource Center: *idtheftcenter.org*
- TraceSecurity, a CUNA Strategic Services alliance provider: *tracesecurity.com*

DON'T GO IT ALONE

Credit unions of all sizes have access to resources to confront growing cybersecurity threats. NCUA, for instance, maintains a cybersecurity resource page on its website that includes substantial guidance, links, and best practices for credit unions to establish a well-considered data security program.

The NCUA's Examiner Guide, the Federal Financial Institutions Examination Council's assessment tool, and the Financial Services Information Sharing and Analysis Center, which provides cyber and physical threat intelligence analysis and sharing.

Plus, many third-party firms provide a range of information technology (IT) security, compliance, risk, and audit solutions. And the CUNA/league system offers multiple compliance resources, including the Compliance Community, compliance training, e-Guide, and CompBlog.

TraceSecurity, a CUNA Strategic Services alliance provider, offers risk assessments, IT security audits, social engineering engagements (both remote and onsite), vulnerability assessments, external and internal penetration testing, wireless access penetration testing, web application testing, and other services.

Two solutions TraceSecurity offers to protect credit unions' data:

- **TraceEDU,** a cybersecurity education platform designed to increase employees' overall security awareness. The platform allows credit unions to assess individual employees' security awareness, and enroll them in customized training as needed. This includes remote social engineering via phone call spoofing as well as email phishing campaigns.
- **PhinPoint,** a new anti-phishing service that identifies, filters, and alerts employees to phishing emails. The service also checks emails for suspicious words, requests for account numbers, and other unusual activity.