CPA
Practice Advisor

TECHNOLOGY

Here is How to Thwart Cyber Thieves Coming For Your Data

While challenges persist, remote workers can keep data secure by following these nine key tips.

Jason Bramwell • Oct. 06, 2022

It has been more than two years since the coronavirus pandemic forced accountants to leave their work cubicles behind for their new home away from home—which was, well, their homes. And even though many public accounting firms and corporate accounting and finance departments are starting to make their employees come back to the office and become familiar with their cubicles again, a lot of these same companies are continuing to allow their staffs to work from home two or three days a week under a hybrid work model—and others have gone the remote route permanently.

But the continued remote work environment has cyber criminals licking their chops, as they look to exploit vulnerabilities in companies' security infrastructures and target employees through phishing emails and other schemes in order to gain access to their login information.

"When you move to remote work, anything that was a potential weakness in your internal control system or your security architecture or your cybersecurity plan now becomes completely apparent; that's when it becomes abundantly clear that you have gaps, either on the functional side or on the security side," Darren Guccione, CEO and co-founder of Keeper Security Inc., said during a webinar. "Because at the start of it, cyber criminals are always looking for ways to capture login credentials. One of the easiest and lowest technology methods of stealing login credentials is through a phishing attack."

According to a 2022 survey of C-suite leaders by HelpSystems, 29% of respondents cited business email compromise or phishing as their greatest concern, but 43% said the biggest danger to their company and data is ransomware or malware designed to steal data or extort money.

Ransomware rears its ugly head

After getting an employee's login credentials, cyber criminals can move within a network to find sensitive data, such as financial accounts and client information. That data can then be sold to identity thieves on the dark web or held for ransom against the victimized firm.

A ransom cyber incident was brought to light recently when two accounting firms were among several victims of a large-scale computer hacking scheme in the United States conducted by three Iranians between October 2020 and August 2022. The three men now face federal charges of conspiracy to commit fraud, intentional

damage to computers, and transmitting demands, according to an indictment unsealed in September.

In one instance, the hackers launched an encryption attack last February and March, causing a New Jersey accounting firm's network to connect with their server. The cyber criminals demanded a ransom of $50,000 and allegedly told the firm, "If you don't want to pay, I can sell your data on the black market. This choice is yours." It is unknown whether the accounting firm paid the ransom, but federal authorities said some of the victims did pay ransoms, while others contacted the FBI or local law enforcement.

The average cost of a data breach for companies increased to $21,659 per incident last year, with most incidents ranging from as little as $800 to more than $650,000. But 5% of successful ransomware, phishing, and other attacks cost businesses $1 million or more.

Ransomware breaches increased by 13% within the last year—representing a jump greater than the past five years combined, according to a 2022 report from Verizon. In addition, external bad actors are approximately four times more likely to cause breaches in an organization than internal personnel.

The Verizon report also revealed that people are the weakest link in an organization's cybersecurity defenses. When you include human errors and misuse of privilege, the human element accounts for 82% of analyzed breaches over the past year, rather than cyber thieves exploiting flaws in computer systems.

In addition, cyber criminals have used the pandemic as an opportunity to capitalize on people's strong interest in coronavirus-related news by luring people to fake malicious websites, clicking on malicious links, or providing personal information online or over the phone under the guise of COVID-19. Many of these scams attempt to impersonate legitimate organizations, such as the Center for Disease Control or the World Health Organization, by offering fake informational updates and even promises of access to vaccines—all for a price. These so-called social engineering attacks accounted for 25% of total breaches in 2022, according to Verizon.

"When there is a mass amount of movement or migration to remote work environments and a greater number of endpoints, as well as a greater level of anxiety, this is as much about the physical and the psychological as it is about just general architecture. It involves everything," Guccione said. "There's a state of panic, there's a state of uncertainty, there's transitioning—there's so much going on that cyber

criminals really gravitate toward situations like this because they always want to attack the lowest-hanging fruit and any companies they view as a potential weakness."

Most common entry points for cyberattacks

Changes in information technology infrastructure brought about by remote work, such as a move to cloud solutions, has shifted the focus of cyberattacks, according to a new report from Hiscox and Atlas VPN.

Cloud servers is now the No. 1 way in for cyberattacks, with 41% of companies reporting it as the first point of entry—a 10% increase from the year before. Cloud servers has replaced corporate-owned servers, which was the leading attack entry point, or vector, in 2021.

Corporate-owned servers now occupies the third spot on the list, according to the report, with 37% of businesses reporting this as the main cyberattack entry method. Meanwhile, the second spot now belongs to business emails, as 40% of companies named it the main access point for attackers.

"If you get a spam email or an email that looks legit but is asking you to do something like upload some information or change a password or even transfer funds, make sure you have a policy in place to make a verbal verification for that. No client is going to be upset if you call them and say, 'Did you really want me to transfer $10,000 to this account?' Because if you do it and you don't call, they are going to be upset if it's not a real request because there's no getting that money back. It'll be gone," Bobby Garrett, IT director at CPA firm Gray, Gray & Gray, said during a virtual podcast.

Employee-owned mobile devices is another common entry point for cyberattacks at 29%, an increase of 6% from the previous year, according to the report. Others include remote access servers at 31% and distributed denial of service (DDoS) attacks at 26%.

"When we all go remote, a lot of traditional internal control policies become less effective and they become dilutive when it comes to exploiting or capturing security vulnerabilities," Guccione said. "And so now as we all move to this much larger endpoint landscape and geometry, we now have to figure out, well, what do we need to do to make sure that we're tracking and monitoring every endpoint—smartphone, tablet, computer—across every employee in the organization? What can we do to

track that down and make sure that on the prevention side of cybersecurity that we're doing what we need to do to protect our environment?"

Strategies for securing data while working remotely

In the two and a half years since the pandemic began in the U.S., companies have been able to fine-tune their cybersecurity processes for remote workers. But the continued number of cyberattacks in the U.S. means IT professionals cannot let their guard down—and neither can a firm's employees.

The following are best practices compiled from articles, reports, and webinars on how to reduce the risk of a data breach in a remote work environment. (Note: This is not an all-inclusive list and the best practices are not numbered in terms of importance.)

1. Ensure you have a modern cybersecurity plan that covers remote work environments: Firms need to make sure endpoint security and enterprise password security software is running on all employee devices, Guccione said.

"We know password security is the trojan horse into your business. So at the end of the day, you could have the best antivirus protection and you could have the best privileged access management system running, but if you do not put a cloak of armor around your password security and your password internal controls and enforcement policies, you are in real serious trouble because this is where the cyber criminals know exists the lowest-hanging fruit. This is where it's at," he added.

2. Use a Wi-Fi password: But do not use the default password, Jim Bourke, a partner at CPA firm Withum and managing director of the firm's Advisory Services practice, said in a video for the American Institute of CPAs.

"If you're using the default password on your Wi-Fi device, change the default password. Go into your Admin settings and make that change," he said.

Bourke also recommends changing your service set identifier (SSID). "What is your SSID? That is your Wi-Fi network name. So change your SSID, make it generic. It will be less likely to be hacked," he said.

3. Install antivirus and internet security software at home: One of the most common—and effective—security strategies for working from home is to invest in a

comprehensive antivirus suite for your company and your employees.

Antivirus suites offer automatic remote work security against a host of threats, including:

- Zero-day attacks (viruses taking advantage of security gaps before they are patched);
- Malware, spyware, and viruses;
- Trojans and worms; and
- Phishing schemes, including those sent via email.

Nowadays, comprehensive antivirus and internet security software automatically updates itself to stay on top of new and emerging threats.

4. Use a VPN: Virtual private networks (VPNs) add an extra layer of protection to internet use from home. They cannot on their own be relied upon to prevent cyberattacks, but they can be a useful barrier against one.

According to antivirus provider Kaspersky, VPN security can be enhanced by using the most robust possible authentication method. Many VPNs use a username and password, but firms might want to think about upgrading to the use of smart cards. Companies can also enhance their encryption method for VPN access, for example, by upgrading from a Point-to-Point Tunneling Protocol to a Layer Two Tunneling Protocol.

But no matter how strong your VPN is, if an employee's password is compromised, it will give hackers an easy way in. So Kaspersky recommends that employees update their passwords regularly. Employees should also be reminded to only use the VPN when they need it, switching it off if they are on their work devices for personal use in the evenings or on weekends.

5. Define clear procedures for reporting and responding to security incidents: "This is so important because if everyone is remote and there's an anomaly or an incident with somebody's email system or somebody in your organization believes that there's been a breach, you want to make sure that they have a well-defined incident response plan so that they can identify, mitigate, and reduce the cost of the cyberattack," Guccione said. "Most importantly, we want to make sure that every person in the organization knows what to do if they think there's been a breach. They need to know who to report it to, how to report it, and what to do. So making sure that you have this plan in place is of paramount importance."

6. Set up two-factor or multifactor authentication: By now, we've all used two-factor or multifactor authentication when logging into something, whether on our work computers or on our mobile devices. Cybersecurity experts say it is an effective and fairly easy-to-understand extra layer of security.

When used with single sign-on solutions, multifactor authentication makes logging in easier because it allows users to pass through many security measures at once.

"When you sit in front of a system that's protected with multifactor authentication, you present a username and password—something you know—and then you provide a PIN from a security token—something you have. This can be a hard token, a soft token, or a smart card," Steve Tcherchian, chief product officer and chief information security officer at XYPRO Technology, said during a webinar. "If you don't have that token, you won't have that PIN. And that PIN, in most cases, will rotate every 30 seconds. So even if your username and password were stolen, unless the attacker has that token along with your username and password, what your PIN was at that moment in time, your username and password is useless to them."

7. Make sure critical applications utilize zero knowledge, zero trust, and end-to-end encryption: Zero knowledge is "the premise that only the user of your application has full knowledge of your master password and complete control over and domain of, in terms of ownership, your encryption key that's used to encrypt and decrypt your information," Guccione said.

"When you buy these products, you want to make sure that any encryption or decryption is done client-side, meaning it is done at the client device level. It is not done at the vendor level," he added. "The vendor should never be generating those keys for you, and they should never have the ability to decrypt and view your information. This is really important."

The premise of zero trust is "the idea around privileged access that you want to make sure in a very simple world you can trust, but you always must verify," Guccione said.

"At the end of the day, you should know through event logging and reporting what every single user on your system on every device is doing, what they're accessing, and who they are transacting with," he continued. "And you should have those internal controls, those role policies, those enforcement policies, the reporting, and the logging, and the auditing capability in that ecosystem to make sure you can lock everything down if there is an incident, whether by a rogue employee or an external

adverse third party or bad actor. You can lock down that device and make sure that you maintain the integrity of your organization."

End-to-end encryption is really important to have for sensitive information, such as personal identifiable information, business assets like a business plan or a financial model, tax returns, or wiring instructions to a bank account, he said.

"If you're transacting over any type of productivity application or security application, you want to make sure all of that information is completely encrypted from point A to point B, and that means from one user device to and through the internet, down into that device and into their screen from A to Z. You want to make sure that you practice full end-to-end encryption," Guccione said. "These three things are so critical because they're intrinsic and existential elements of any great productivity and security application."

8. Provide cybersecurity awareness training that includes threats and best practices: Guccione said it is extremely important that every single person in the organization who uses a computing device is trained on things like phishing scams, cybersecurity awareness, the dark web, and credential stuffing attacks. He added that phishing simulations "are one of the best tools that you can utilize in a company to prevent against a password-related data breach."

9. Keep family members away from work devices: Kaspersky recommends reminding your staff to not allow other household members to access their work laptops, mobile devices, and other forms of hardware. They should also be reminded of the importance of password protecting their devices to prevent third parties from accessing sensitive files.

Bourke recommends setting up a separate network in your home for guests. "Do your work under your secure Wi-Fi network that you have in your house, and if you bring guests over, set up a guest network. Guests should use that network and have that password. It keeps things totally separate," he said.

Jason Bramwell is senior staff writer for *CPA Practice Advisor*. He has nearly 25 years of professional writing experience, the last nine covering the accounting profession. He most recently was a staff writer and editor at Going Concern, and he previously spent five years as a staff writer and editor at AccountingWEB. He can be reached by email at jbramwell@cpapracticeadvisor.com.

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.