accountingTODAY

PREMIUM TECHNOLOGY

Cybersecurity: Securing your firm's perimeter

By Antoinette Alexander November 22, 2023, 9:00 a.m. EST 13 Min Read

How safe is your client data? This is a question accounting firms of all sizes must consider as data breaches remain a real concern, and new and emerging threats take security worries to new heights. Accounting firms are the gatekeepers to a treasure trove of sensitive client data, which makes them a highly attractive target for hackers.

"Given the sensitive nature of the data that they process, they are a target. They have financial information; they have tax information. So, the bad actors are looking for them," said Shane Bratvold, a senior director and business information security officer at Thomson Reuters.

Echoing the sentiment, Molly Gallaher Boddy, senior product marketing manager for security at Rightworks (formerly Right Networks), said, "I think that small and medium businesses are the biggest target for cyberattacks and then, when you look at firms specifically, they have the type of data that attackers really want. Think about what you can access from an accounting firm, and compare it to other industries: It is a rich data source for attackers. And I think attackers know going in that those firms are unlikely to have those enterprise-level, layered protections that they expect to find with larger companies regardless of their industry."

According to the "Q3 2023 Data Breach Report" by the Identity Theft Resource Center, it tracked 2,116 publicly reported data compromises across numerous industry sectors through the first nine months of 2023 — breaking the all-time high of 1,862 compromises in 2021.

Furthermore, the report found that cyberattacks remained the most common root cause of a data breach in Q3 (614 breaches). Among those that reported an attack vector (which is the method in which attackers enter a network or system), phishing attacks were the most frequently reported cause, totaling 80. This was followed by:

- Zero-day attacks (attacks against a previously undisclosed software flaw for which there is no patch) — 69;
- Ransomware — 64; and,
- Malware attacks — 17.

What is especially alarming is that financial services topped the list as the most attacked industry. According to the ITRC report, the number of financial institutions reporting data compromises soared in Q3, with 204 notices issued. This exceeded the total number of financial service compromises reported in the past two years.

accountingTODAY

PARTNER INSIGHTS FROM INTUIT QUICKBOOKS

Accounting firms have a fiduciary duty to keep client data safe and secure, and federal law requires all professional tax preparers to create and implement a data security plan. Security breaches not only jeopardize a firm's reputation but can also result in monetary penalties and even criminal liability. This is a risk firms cannot afford to take.

accountingTODAY

accountingTODAY

According to data provided by Statista, the average cost of a data breach in the United States reached $9.48 million in 2023. This can include things such as legal fees, remediation, lost revenues, ransom payments, etc. According to *Accounting Today*'s "Year Ahead" survey, cybersecurity risks ranked as the leading technology concern for firms (53%) in 2023.

Firms no doubt recognize the importance of data security. However, for many, the question is, how can they successfully secure their perimeter?

"Often what I hear from a firm director, or a firm general manager, or managing partner is they are aware they are not as secure as they need to be but, one, they don't know where to start; and, two, how to get there; and, three, do they have a vendor that they can work with that will help them get there," said Christopher Stark, founder, president and CEO of Cetrom, an IT provider of custom cloud hosting solutions for accounting firms.

The leading threats

As technology evolves, so do the tactics that attackers employ to steal and monetize data. For firms, keeping pace can be easier said than done. According to industry sources, the leading security threats facing firms today include phishing and spoofing, and ransomware attacks.

1. Phishing and spoofing. Both attacks employ social engineering tactics to deceive people into taking an action and disclosing sensitive information. While phishing and spoofing are related concepts, there is a difference. Phishing is a type of attack, while spoofing is a means for making attacks like phishing more believable. For instance, when performing a phishing attack, a cybercriminal may use email spoofing to make that malicious email more believable and trusted.

In a recent statement, the IRS said it continues to see a "steady stream of attacks" against tax professionals as hackers look to steal sensitive tax and financial information from their clients. Among the most common threats facing tax professionals: phishing and related scams.

2. Ransomware and malware attacks. Ransomware, which is a type of malware, can be especially devastating and costly for firms should they fall victim to it. As the name suggests, these attacks essentially hold a firm's data and devices hostage until a ransom is paid. A 2022 Small and Medium-Sized Businesses Ransomware Survey sponsored by CyberCatch, a cybersecurity software-as-a-service company, found that roughly half (48%) of accounting firms said they would survive only three days from a ransomware attack. Furthermore, 31% said they have no backups offline.

In prior years, ransomware attacks basically demanded a ransom in exchange for an encryption key needed in order for the victim to regain access to the affected data or the use of the infected device, as explained by IBM. Companies could mitigate, or maybe even eliminate, the risk of paying a ransom with regular or continuous data backups. However, the ransomware attacks have now evolved into an even more dangerous and damaging threat: double-extortion and triple-extortion attacks.

accountingTODAY

According to IBM's 2022 report, "Cost of a Data Breach," the average cost of a data breach caused by a ransomware attack — not including the ransom payment — reached $4.54 million. And, according to a 2022 Cyber Protection Operation Centers Report by Switzerland-based cybersecurity company Acronis, global ransomware damages are estimated to exceed $30 billion in 2023.

Said Stark of Cetrom, "By far, the most detrimental, damaging component of an attack is, for example, a cyberattack like a ransomware attack or a highjacking, if you will, extortion, because now what's happened is the threat has evolved."

Securing your perimeter

It is critical that accounting firms have rigorous security measures in place to safeguard data and protect their business from the threats. However, given the advancements in technology and evolving tactics being employed by attackers, it can be challenging for firms to determine how to best secure their perimeter. For some firms, navigating the complexities can seem daunting.

While firms may not be 100% safe from attacks, there are undoubtedly some critical basic steps they should immediately take to maximize security. As outlined by the American Institute of CPAs, these include:

1. Enforcing password policies. This means professionals must use complex passwords and frequently change their passwords (at least four times per year). Leveraging password managers can help staff adhere to these policies. How? Password managers create an encrypted storage space for all of the user's passwords. This frees staff from having to track all the complex passwords they've created.

2. Using multifactor authentication tools. MFA tools need to be used at all levels for everyone accessing data, and must be implemented on all devices, including cell phones. This adds another layer of identity verification to the sign-in process and makes it harder for hackers to access vital information. MFA relies on the verification of two or more factors:

- Something you know (i.e., your user ID and password);
- Something you have (i.e., your mobile device, etc.); and,
- Something you are (i.e., your facial image or fingerprint).

3. Minimizing access to necessary levels. This means restricting the number of users with administrator privileges and setting access levels to the minimum level required by each user to complete their work. It is important to regularly monitor and evaluate access, and terminate it when the access is no longer required.

"I think there's a lot of fairly basic things accounting firms can do that can significantly increase their security posture and, in turn, reduce the risk of them falling victim to a cyber attack," said Thomson Reuters' Bratvold. "Have a good password; change your password on a regular basis; use MFA; have a security policy, and train your staff on it. Those are fairly basic things. Yes, they will take work, but if you do the basics you reduce your risk a fair amount."

perimeter is unclear. In the past, the perimeter was the internet and your network, but now with cloud-based applications, with remote work, that perimeter has a lot of entrances and you need to look at all of them when you do this assessment," Rightwork's Boddy said.

She continued, "If I were to go through the layers, I would definitely start with the application layer. I would look at how your applications are being accessed. I would take a look at your infrastructure, which is obviously related to how those applications are delivered because the security of your infrastructure requires a great deal of management, and do you have the resources to appropriately manage that infrastructure? And then you can start to go out to devices. How employees are using those devices both during the workday and on their personal devices, and then going to other threat vectors such as email, for instance."

In today's tech-driven, interconnected environment, it is important to be aware of all of the places the firm's data may potentially live. Stark agreed that conducting a risk assessment is critical and also stressed the importance of hiring an independent firm to "come in and do a boots-on-the-ground approach of looking at your security posture" versus just running an automated scan to identify potential vulnerabilities.

"It starts off with: Where is your data? Where are the assets of the organization, which is usually the data. Start there, and: How are we protecting that? What methodologies do you have in place? What automation of updates are you doing on all your assets? Are you following the least-privilege model? Are you doing backups on your data?" said Stark. "Based on that data and that feedback, you are going to understand: Where are my threats? Where are my assets? What am I doing to protect them? What measures do I have in place? Am I following best practice for doing patching and updates? Do I have an NGAV [next-generation antivirus] in place that is protecting them? Are user accounts two-factored? These are things that are complicated."

Industry sources also recommend that firms adopt a "zero trust" approach and invest in staff training to help eliminate internal weaknesses and human error. Zero trust is a framework that assumes every connection and endpoint is a threat, regardless of whether it is internal or external. As explained by IBM, a zero trust network, for instance:

- Logs and inspects all corporate network traffic;
- Limits and controls access to the network, known as least-privilege access;
- Verifies and authorizes every connection, such as when a staffer connects to an application programming interface; and,
- Authenticates and authorizes every device, network flow and connection.

When asked about staff training, Jamie Simmons, the chief information officer for Seattle-based Top 100 Firm Moss Adams, stressed the importance of continuous security awareness training among end users. "We do that in a couple of ways. One, we have our annual, required security awareness training for all individuals. … If you don't get [the training] done, eventually your access is locked and you can't log into the network until you go through it," said Simmons. "The other way is we run phishing campaigns regularly. Our IT security team is constantly, as bad actors, trying to come up with creative ways of tricking our end users into progressing through a series of [phishing attempts] all the way through, in some cases, putting in login credentials, which obviously sets off a big alarm for us. We are tracking and monitoring that to see if we are improving in educating folks."

It is also critical to not underestimate the importance of having a written security plan in place. In fact, federal law requires all professional tax preparers to create and implement a data security plan. Enter Publication 5708, which has been worked on by members

accountingTODAY

"It really gives you a step-by-step way to go about starting down this path and this process of creating a plan and taking your inventory, looking at your data disclosures, understanding your network protections, creating policies around these things," said Shannon Bond, vice president and segment leader for the U.S. preparer market for Wolters Kluwer, who took part in the development of Publication 5708. "We tried to do it in a very user-friendly way that lets you dip your toe in the water and get started."

There is no one-size-fits-all approach to developing a written information security plan. It should be appropriate to the firm's size, scope of activities, complexity and the sensitivity of the customer data it handles.

Generative AI: An emerging threat

As technology evolves, so do the emerging threats, as evidenced by the rise of generative AI, a form of artificial intelligence that can perform such tasks as creating original articles, music and code. Among the most talked about is ChatGPT, a sophisticated, next-gen chatbot.

Generative AI has the potential to significantly impact the profession; however, the industry is undoubtedly treading very cautiously. Among the greatest concerns: privacy, data security, confidentiality, and loss of autonomy or control.

"At large, what practitioners and firms need to consider is just the data privacy and the confidentiality of these public [platforms], like ChatGPT, for example. They all have varying terms of privacy and confidentiality, and you don't know what they may be or won't be, and you have to watch for … any kind of data leaks or things that you may put in there or inputs that it's learning from," Bond said.

Stark agreed and said, "I'm in the IT field and I've seen a lot of things come and go. It is, by far, one of the most interesting that has come out of the IT field in many, many years since the internet came out, but is it mature? Is it regulated? Is the information accurate? Whose data is that now? I think we are in the infant stages of that technology becoming a standard."

Underscoring the point, recent research by Thomson Reuters Institute found that nearly 70% of tax professionals said their firms or departments had risk concerns surrounding the use of ChatGPT and generative AI.

Said Bratvold, "Some advice for accounting firms is to educate themselves on it. Read up on it. If they have an IT department, or a security or data privacy department, they should be educating themselves on it, and, ideally, they are defining some sort of acceptable use policy within their firm."

Antoinette Alexander

TECHNOLOGY CYBER SECURITY PHISHING CYBER ATTACKS