If you don't have one, you should work with your legal counsel and other specialists to ...

Jun. 13, 2016

Imagine this. Your firm starts receiving calls and emails from clients saying they've been the victim of tax refund identity theft. Sure, you've seen a few of these cases and have a process in place to assist clients, but this appears to be different. The volume of victims is far more than what you'd ever expect.

When you explore the activity on your network, you discover that access has occurred at odd times. Or, some of your partners or staff recall "kicking someone off" the network before they could log in. The client calls and emails begin to accelerate. You ask your staff and partners if they've responded to an odd email or opened an unusual file that seemed to be from a trusted source. You find that they have.

[This article first appeared on the Thomson Reuters blog.]

Your firm has been the victim of a spear phishing attack and someone—or a group of people—have all of your firm's data. Don't think it can happen to you? Think again. This doomsday scenario is happening to firms of all shapes and sizes, and the number of occurrences is rising.

How it happens

In many instances, malware that can track keystrokes is residing on an office PC or on your firm's network. The result? The hacker(s) now have legitimate credentials from one or more of your staff. They go freely in and out of your system like legitimate users. And they know what to look for—full tax returns or W-2s from your payroll services, as well as business financial data. To tax refund thieves, this is a gold mine because it's real data—employers, addresses, dependent names, ages, Social

Security numbers, etc. With this data, producing W-2s that look legitimate and then

If your systems have been compromised, there are a number of steps to take immediately. These actions should be outlined in your firm's incident response plan. If you don't have one, you should work with your legal counsel and other specialists to develop one immediately. At a minimum, your Incident Response Plan should require that you immediately take or at least consider the following actions.

Note that I'm not a lawyer, so this is not intended as legal or tax advice if you find your firm in this situation. Instead, view these as general guidelines.

1. Your information security team and forensics specialists should quickly determine if you must quarantine any or all of your PCs or other devices, and your network. Because the malware is residing somewhere in your system(s) and will still track keystrokes, simply changing passwords is pointless. If you don't eliminate the root cause, the process can start all over again. The malware essentially "owns" your technology until you hire a professional to remove it. It is also important to note that once you know there's been a security breach, you should assume that the thieves accessed all of your client's data (and employee data, if you do payroll).
2. Contact your attorney and request a reference for someone familiar with data breach regulations. Your insurance carrier may be able to assist with this as well. Legal counsel is a very valuable resource in assisting with the overall management of the incident and engaging with third-parties like law enforcement, forensics, insurance, etc.
3. Have the computer forensics expert assess what was accessed and when.
4. Notify all staff that until a communication plan is established, and you truly understand what occurred, that the situation is to remain confidential.
5. From the known access point, start compiling the list of clients and/or employees whose personal or confidential information may have been accessed. Also determine the states in which these clients and/or employees reside as that will help your legal advisors determine whom must be notified of the incident and by

when. It is critical to get the notification process and timing right, and the

about how this occurred.

10. Contact the state regulatory authorities if required.
11. Develop your plan for personal contact of key clients, including an escalation process if you receive a negative reaction.
12. Ensure that all partners and staff have the same script for all related client interactions.
13. Assign one person to be the external spokesperson for the firm—your press relations person—and ensure that person has a solid script for any comments. You may also need to draft a press release.

Once again, this list is not intended as legal advice—it is merely a list of suggestions that illustrate some of the action items involved in responding to a data breach. This list is not all inclusive, but rather a general guideline. You should contact an attorney for advice on legal matters.

While this list of action items may seem intimidating, the situation calls for immediate action and total focus. The keys are quarantining your technology, bringing in the forensic experts to assess the damage, contacting your attorney who should be able to assist with engaging with third parties, including managing any notification process and its timing, and building the internal and external communication plans. Remember to remain calm. If you can show that you took immediate, direct action, documented the incident and remediation steps, and engaged the appropriate third parties for assistance, your outcome will likely be the best possible. If you hesitate, or resist what needs to be done, the outcome may not be as good.

Obviously, the firm needs to continue operating while all this activity is going on. In parallel with the forensics analysis, have new stand-alone PCs up and running with the applications you need to serve your clients and to run the practice. The forensics results will determine what occurs next with your environment and network.

How to protect your firm against hacking

malicious links in email, attachments and social-engineering attacks. So, if you haven't asked your internal IT staff or your outside consultant about targeted threat protection, you should do so ASAP.

Other reference guides on data security include IRS Publication 4557 and the FTC's guidance on security..

Unfortunately, cybersecurity is now a priority for all of us, particularly those of us in the accounting profession who hold so much personal and financial data for our clients. You owe it not only to your clients, but to your employees and yourself, to take this threat seriously and protect your firm in every way possible.

———

Jon joined the Tax & Accounting business of Thomson Reuters in 1992. Prior to his current position as Managing Director of the Professional segment, Jon held the positions of President of Professional Software & Services, and Vice President of Development, where he was responsible for the design and development of all Professional products and services. Jon has three decades of technology development and management experience, including 17 years with CCH Computax (now the Tax business unit of Wolters Kluwer North America) in various executive technology development and operations positions. Jon holds a BBA in Accounting from Siena College and an MBA from Boston University.

Firm Management • Security • Technology