BULLIVANTHOUSER

Wilhelm Dingler
Seattle, Shareholder

Direct Dial: 206.521.6409
Fax: 206.386.5130
Email Attorney

Risk Management Protocols: First Step against Cyberthreats

By Wilhelm Dingler

Wolters Kluwer, the provider of the CCH Tax Software suite of products, discovered an "anomaly" in the spring of 2019 that, upon further investigation, was determined to be malware infecting its systems. The company immediately took its systems off-line, and they remained so for over three days. Not only was access unavailable for most tax practitioners, many accountants began to ponder the question, "Do I have to do the data breach notification protocol mandated by my state?" Moreover, there was consternation in the profession concerning what this incident might mean for them in terms of liability exposure. The incident, as unhappy as it was, serves as a good learning moment to emphasize some risk management tools CPAs can use to protect themselves from liability exposures in the digital age.

Wolters Kluwer had third-party forensic consultants investigate. There did not appear to be any specific indicators that a data breach actually occurred or that any client data or personal information had been compromised. The reason the company was able to immediately cap any potential issues is because it had a plan in place. When it comes to CPA firms, implementing safeguards and protocols is a must, and they should be tailored to the unique circumstances of the firm's practice size, scope, client base, and other factors. There are, however, some general tools to employ to better forestall digital breaches or respond to ones that do occur.

Perhaps the best "tool" to avoid falling victim to online criminals is vigilance and forethought. All criminals seek low-hanging fruit in their efforts. Most don't expend the effort needed to attempt a hack of Bank of America; they go after actionable information in the hands of CPA firms. Many will pretend to be your client requesting an activity, so your internal protocols and procedures must help thwart such activities. Here are some risk management suggestions in that regard:

- Establish client-approved disbursement procedures
- Use alternative methods to confirm client requests
- Request client's approval at least three business days in advance of payment
- Establish procedures for unusual transactions (in particular, wire transfers)
- Respond to requests using telephone numbers and email addresses from the firm's database (not what may be provided in a call or email)

You may also wish to consider protecting yourself with engagement letter modifications. As an example, for liability insulation from email hacking, consider including language such as the following:

The procedures for email communication and instructions will be provided by the client. The client waives any right against the accountant for "inadvertent" email incidents (as outlined in the client instructions). The client retains all rights and claims for the volitional act of transmitting email(s) to a working email address, but which is not an address associated with or approved by the client. This waiver encompasses only acts beyond the control of the accountant or its personnel (i.e., email hacking or interception, malware, network or IP provider error, theft, and the like), and does not waive liability for negligence in hitting "send" to the wrong person.

Many risk management techniques are common sense. Unfortunately, common sense often takes a back seat when deadlines loom or it is very late in the day on April 14. These are situations cybercriminals seek. It is for this reason that having risk management plans in place and procedures to follow can greatly reduce or eliminate incidents.

Here is an example. An email arrives late in the business day from a client requesting that the CPA transfer funds. The email expresses both urgency as well as a veiled threat. ("We are going to lose this multimillion-dollar deal if you do not get the money wired forthwith to Beta Inc.") The threat is that you will be responsible for the client losing out on this deal. Spoofing, false legitimacy, and a false sense of urgency combine to put the CPA in a very precarious position. To the untrained eye, the email may look legitimate and the request seem logical. This is particularly true if the cybercriminal has just enough information to make everything seem proper – such as the name-drop of a real entity with whom the client does business. ("We obtained a referral to this deal with Beta Inc. from Acme Inc.") As its CPA, you know that Acme Inc. is a large source of the client's revenue.

With a protocol in place, this situation can be avoided. Just as many of us sign into our electronic devices with dual-factor authentication. Using set protocols and procedures, coupled with unwavering adherence to them, is the functional equivalent of dual-factor authentication. Having these established protocols can help you to avoid liability.