AICPA Private Companies Practice Section

AON Empower Results®

HACKED! Building defenses against and responses to intrusion

Cybersecurity and the associated risks to business and reputation are top of mind for CPAs and CPA firms across the United States. Firms put procedures in place to keep information and their systems secure, but what do firms do if they believe a cyber incident has occurred? Here are some key action items firms should take to minimize their exposure and adequately respond to an incident.

Aon strongly recommends working with various professional experts to develop a formal incident response plan and to test the plan on a regular basis so that when a breach occurs, you're ready and can respond in an informed way. Secure relationships with key vendors before an incident so there is not a scramble to find resources at the time an incident is discovered. Being unprepared can be costly and the longer it takes to understand the scope of a breach and remediate, the more expensive the incident becomes and the greater the potential of harm to your firm's reputation. While the extent of each breach is different, and some will be simpler to respond to than others, all the areas below should be considered when developing an incident response plan and used as a checklist if a breach has been detected.

1. Contact insurance carrier or advisor:

If you have a cyber policy in place in the event of an actual or suspected incident, the first thing to do is contact either your cyber carrier or insurance advisor. A strong cyber carrier will have the resources in place to assist you with forensics, legal, notification and post breach services, public relations (PR) experts and IT consultants. If you do not have a cyber policy in place, it is a best practice to have vetted contacts in the following specialties: forensics, legal, call center and notification services, public relations, IT cybersecurity and data, credit monitoring, and regulatory and law enforcement.

2. Utilize forensics specialists to identify breach details:

If a suspected or known incident has occurred, the extent and scope of the hack or breach must be determined. The Ponemon 2017 Cost of a Data Breach study indicates that it takes an average of 191 days to identify a breach. Forensics experts help determine how long ago the breach occurred, how the breach occurred and what data has been exposed.

3. Consult with applicable legal experts/regulators:

Once it has been determined that data has or potentially has been exposed and to what extent, the legal experts will be able to determine what needs to occur next. The resident state of an impacted individual is the applicable state law for that individual. Each state has various requirements based upon the specifics of a breach including how notifications need to be communicated. Attorneys that specialize in data breaches will be able to assist with this as well as understanding if credit monitoring must be offered. If not required by law, there is always the option for voluntary notification and credit monitoring due to the specifics of the breach to help reduce loss of clients or harm to a business's reputation. In addition, there may be a requirement to inform various regulatory bodies depending upon the location and circumstances.

4. Complete required notifications and/or credit monitoring:

As noted above, attorneys specializing in data breaches can help with the notifications and determining if credit monitoring is required. Whether mandatory or voluntary, a credit monitoring provider will need to be obtained. Notifications will also need to be mailed and a call center needs to be hired or established with firm staff (who will need to be trained and dedicate time to take on call center responsibilities) to handle calls/complaints in response to the content of the notification and the breach.

5. Take steps towards remediation:

What caused the breach in the first place? If it was human error, additional training may be required. Regular training is one of the best prevention methods. If there was a systems issue, perhaps IT consultants need to be hired to help provide the guidance needed to secure the current system or install possible upgrades in security software.

6. Restore data:

A good measure is to back data up on a regular basis. This will alleviate some of the time spent in trying to recreate lost or stolen data. Failure to backup data regularly may result in IT consultants tasked with helping to restore lost or stolen data which could disrupt business.

7. Manage public relations to protect your firm's reputation:

Depending upon the extent of a breach, a PR firm may need to be retained. Time is money so getting in front of a situation as quickly as possible can help mitigate reputational harm and lost business. Having PR professionals will assist in getting your message out promptly and effectively. Securing this relationship in advance can help the PR firm become familiar with your firm and its culture so that in a crisis situation, the PR firm is better prepared to help you respond.

8. Involve law enforcement:

It is recommended that you have a relationship with the Local FBI Field Office prior to a cyber incident. A firm can contact the local FBI office directly or go through an attorney that specializes in data breaches. The FBI can describe the current cyber threat landscape and provide an understanding of how they're able to assist in the event of a data breach.

No CPA firm wants to be a victim of a cyber breach but unfortunately, even highly protected data can get into the hands of criminals. Being prepared will help any firm in the event of a worst-case scenario. Use these tips and the types of professionals mentioned above to help prepare your firm's response plan for cybersecurity events.

This information is provided for general informational purposes only and is not intended to provide individualized business, insurance or legal advice. You should discuss your individual circumstances thoroughly with your legal and other advisors before taking any action with regard to the subject matter of this article.