

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

for criminal hackers. They are like an auto accident waiting to happen.

Jan. 20, 2014

Accounting firms are repositories of personal information and have become targets for criminal hackers. They are like an auto accident waiting to happen.

When you have a serious automobile accident, you have to report the accident to the local authorities. The police could make a determination as to who is at fault and citations and fines could be issued. Of course, you want to report the accident to your insurance carrier to protect yourself from litigation and you want to repair your vehicle. At some point, a determination is made as to who was at fault and who has the greatest liability; attorneys on both sides are always involved.

You will be asked for your current insurance card, your up-to-date license and registration. Your inspection sticker will be examined. You will have to show that all your records are up to date and in compliance with your state laws and regulations.

What happens when you have a Cybersecurity data breach? Once you have recognized your accounting firm has experienced a breach, under the Notification laws in 47 states you have to notify state authorities, in most cases at least two agencies and in some cases, three. If your firm conducts business in multiple states, perhaps even more. You will need to contact an attorney who specializes in the Privacy area to guide you thru the maze of requirements and defend your firm. You will have a definite and specific time limit to accomplish the state regulatory notification requirements, and prepare to notify all employees, clients or other affected parties. This is usually 60 days. Once you have notified the state or states you will probably notify your insurance carrier because of the potential litigation, losses and damages your enterprise could be subjected to. At this point reputation management becomes a serious issue.

The accident/breach has happened and you have reported it so be prepared for a

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

and limit firm or personal exposure: Insurance (liability/collision), proper maintenance, state inspection up to date, registration and license up to date, driving classes and more.

What are you doing in the Cybersecurity arena to develop a defensible breach approach to manage and limit your potential exposure?

Reports are showing that the number of breaches effecting accounting firms and small enterprises are rising dramatically while the number of breaches effecting very large firms and enterprises are dropping. Large firms and enterprises have the manpower, expertise, money, and resources to develop cyber policies and defensible breach procedures. Small accounting firms and enterprises do not, so the criminal hackers are going where entry is easiest and most profitable for them, easy entry because controls are not in place.

What you have done in regards to your firm's systems and what you are doing concerning the incident could be looked at very carefully. The actions your firm takes because of a breach could be closely examined. Your firm needs to be prepared for this eventuality. Like disaster recovery plans that are becoming more popular for firm as a result of climate emergencies, Defensible Breach Response Plans and WISP Plans are necessary for the reality of regulatory and/or litigation scrutiny.

Criminal hackers, when breaking into firm's systems, will often leave proof they were in your computer system and show they have had or can have complete access to personal information as well as sensitive data/intellectual properties. In today's environment, your firm could expect a federal or state regulatory agency visit and there could be a class action suit or some type of litigation as a result... as has happened repeatedly in recent months.

---

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

CPA Practice Advisor 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.

© 2024 Firmworks, LLC. All rights reserved