CPA
Practice Advisor

CONTRIBUTORS

You've Been Breached. Now What?

Identity theft is the fastest growing crime in America and accounting firms, with their wealth of taxpayer personal information, are often ground zero for cybercriminals. For many, the question is not if you'll be the target of a cyber-attack, but when.

Jim Boomer • Oct. 10, 2017

Identity theft is the fastest growing crime in America and accounting firms, with their wealth of taxpayer personal information, are often ground zero for cybercriminals. For many, the question is not ***if*** you'll be the target of a cyber-attack, but ***when***. And while prevention is of primary importance, your firm should also have a data breach response plan in place for when the unthinkable happens.

Act fast

A rapid response is critical, which is why you need to have a response plan in place before a breach occurs. Most states have data security laws that require firms to warn affected clients within a short time. Contact the IRS Stakeholder Liaison for your state for up-to-date instructions.

Secure your systems and physical areas

Move quickly to secure your system and fix the vulnerabilities that caused the breach. The exact steps you'll take here depend on the nature of the breach, but take any steps necessary to ensure it doesn't happen again. Your IT team should quickly determine if you need to quarantine computers or other devices. Don't turn any machines off

until forensic experts arrive. You may need to update the credentials and passwords of authorized users, but if malware is in your system tracking keystrokes, simply changing passwords is pointless.

If the breach involved your physical premises, you will need to change locks and access codes.

Notify law enforcement

Contact the FTC and your local police department immediately. The sooner law enforcement is made aware of the theft, the more effective they can be.

Assemble your breach response team

You should have a list of internal and external personnel and resources readily available. Depending on the size of your firm, this may include IT, human resources, communications, and management. You might consider hiring an independent forensic investigator to help you determine the source and scope of the breach.

Engage your communications plan

Your communications plan should reach all potential victims including employees, clients, technology partners, and other stakeholders. Don't make misleading statements about the breach or withhold key details that could help clients and employees protect themselves, but don't publicly share any information that could put them at further risk.

Notify all staff that until your communications plan is established, the situation is to remain confidential.

Part of your communications plan should be anticipating questions that people will ask. Good communication up front can help alleviate client concerns and frustrations, saving you time and money later. One person within your firm should be the designated point person for releasing information. Give that person the latest information about the breach, your response, and how individuals should respond.

Notify appropriate parties

Many states have enacted legislation requiring notification of security breaches involving personal information. Your legal counsel can also help advise you on

federal and state laws that apply to the breach.

Consult with law enforcement about the timing of the notification so it doesn't impede the investigation. You should also notify the revenue departments and attorney general's office for each state in which you prepare tax returns.

Offer credit monitoring or other support

If client or employee financial information or Social Security numbers were exposed, consider providing a year of free credit monitoring or other identity theft protection service.

Consider cyber liability insurance

Cyber liability insurance policies can be stand-alone or part of your other insurance coverage program. The coverage it provides varies widely, but policies typically cover the costs associated with data breaches and cyber-attacks, including

- Data loss restoration
- Responses to civil lawsuits
- Payment of government fines or penalties
- Credit monitoring services for clients

Before you purchase the coverage, pay close attention to the exclusions listed in the policy. This coverage will need to be in place *before* you discover the breach. Inform your insurance carrier of the security breach as soon as possible. They can offer more guidance on responding to the breach.

Implement your continuity plan

Your firm can't shut down while you're responding to this attack, so develop and test a continuity plan to ensure the firm can continue serving clients.

This list is not all-inclusive, but it does illustrate some of the actions you should consider when designing your data breach response plan. Responding to such an event may seem intimidating, but the situation calls for immediate action and complete focus. When you can show that you took immediate, direct action and took steps to protect clients and employees, your outcome will be the best in a bad situation.

Cybersecurity is now a priority for everyone in the accounting profession. You owe it to your clients, your employees, and yourself to take the threat seriously.

Contributors • Firm Management • Jim Boomer • Technology • Article

CPAPA 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.