CPA
Practice Advisor

FIRM MANAGEMENT

Why Preventing Data Breaches Should be a Top Priority for CPA Firms

Financial services organizations have been among the biggest targets for hackers in recent years, and it's easy to see why. As keepers of sensitive personal and financial information, CPA firm databases are enticing treasure troves for tech-savvy ...

Jodi Chavez • Jan. 28, 2020

Financial services organizations have been among the biggest targets for hackers in recent years, and it's easy to see why. As keepers of sensitive personal and financial

information, CPA firm databases are enticing treasure troves for tech-savvy thieves looking for a convenient one-stop-shop to plunder. If your CPA firm has been breached before, you're likely already familiar with the toll it can take on both your client relationships and your bottom line. And as these incidents start to increase in frequency, so, too, are the costs. As of last year, the average total cost of a data breach in the U.S. was $8.19M —which is the highest cost globally when compared to other countries.

If you don't have the proper security precautions in place, you could get hit with some pretty steep charges down the line should your clients' data get compromised. And that's not all the damage cyberhackers can do. Here are some additional reasons why your firm should prioritize cybersecurity today — and what you can do to start moving toward achieving the un-hackable ideal.

Damage to your client relationships

Your CPA firm needs clients to thrive, but data breaches of any size can do significant harm to your ability to retain them. A recent IBM report shows firms are more likely to lose clients to a competitor if they experience a data breach. Businesses experience higher customer turnover in high-risk industries. The same study shows churn rates for financial services companies were second only to healthcare organizations at a little over six percent after a breach. Trust is everything when dealing with a person or company's financial information. And once that contract between client and provider is breached, it can be hard to repair the damage. There's no shortage of other firms for clients to switch to in the wake of data theft. And while data breaches are caused by unfortunate circumstances rather than intentional negligence, it's hard to blame clients for wanting to work with an organization with a better track record of security.

To preserve your existing client relationships and position yourself for continued new business, make data security synonymous with your firm's customer-facing identity. Cyber risk governance must start at the top with active participation from the board, and work it's way down to all employees before it can take hold as a permanent feature of your firm's culture. Once controls have been implemented, broadcast the lengths to which you've gone to institute best-in-class controls over protecting your clients' sensitive information. If you've been subject to a data breach in the past, use it as a learning opportunity and showcase how your firm has emerged from the event stronger than before. With your weaknesses now identified and potential vulnerabilities patched up, there's a strong case to make that your firm is now more secure.

Threat of legal repercussions

Remember that 64 percent of customers who said they would stop working with a company if their financial or personal information were stolen? Well, an additional 94 percent of them would take it even further and consider taking legal action against a company whose servers were hacked. We've already talked about the indirect costs CPA firms can suffer at the hands of data breaches by way of fewer customers, but the threat of lawsuits and associated legal fees loom just as large.

While it's true that it's been traditionally difficult for a plaintiff to win these kinds of suits — it's tough to prove, after all, just where exactly an identity thief first acquired the information they ultimately used — there is some precedent. In Krottner v. Starbucks Corp., the court ruled that even just having personal information stolen was considered harmful enough to warrant damages, regardless of whether or not the information acquired was actually misused. As finserv cyber attacks continue to grow in frequency, customer sentiment appears to be reaching a breaking point, and we could start seeing more data-breach victims come forward to press charges against organizations that lose their data.

To protect your firm, institute a formal Enterprise Risk Management (ERM) program and widen its scope to encompass cyber risk. A well-organized ERM program consists of three major components: Risk assessment, risk mitigation and risk monitoring. Defining each of these stages clearly and following the steps associated with each one will put your firm in the best position to ward off potential cyber threats. Here's how to structure your cyber risk management program:

Risk assessment: Conduct periodic evaluations focused on identifying major areas of weakness that could make your firm vulnerable to hacking. Address any control gaps and deficiencies as soon as you uncover them. Review your checks and balances to make sure that your control policies and procedures are still current and effective.

Risk mitigation: Focus on training as well as talent recruitment and retention. Your firm's ability to mitigate risk is directly related to your employees' ability to execute the proper internal control procedures that you established during the assessment phase. That way, when threats arise, you'll be able to respond and report on them quickly.

Risk monitoring: Appoint a dedicated chief risk officer (CRO) who's well-versed in the detailed analytics needed to monitor your program effectively. Instruct internal audit teams to launch compliance reviews and operational audits on a regular basis to make sure your safety controls remain effective.

Upfront protection costs less than accrued theft damages

If you still need convincing about the importance of instituting a cyber risk management program, just look at the latest numbers. The average cost for a lost or stolen record is $242, which has nearly doubled over the last year alone —and continues to rise. Multiply that by every file in your system (plus all potential legal fees we just discussed), and the costs can add up quickly. Investing in data security from the get-go can save you big down the line, and with CPA firms being a top target for hackers, it's an investment you'll want to make. When it comes to hiring the best people for the job, spare no expense, and make sure that the technological safeguards you implement are both top of the line and up to date. Educate your staff on common cybersecurity risks so they know what to look out for, and create clear and defined channels where staff members can report suspicious activity as soon as it's been spotted.

Skimping on immediate IT resources or looking for ways to cut costs in the areas of security may save some money up front, but they make your organization more susceptible to breaches in the end. And if a breach happens, then you may be left with a slew of lawsuits and negative reviews on your hands that could dramatically outweigh the costs you saved from trying to keep your security operations lean.

All employees must be alert to spot potential attacks

It's not only your data security team that needs to stay on their toes. Mitigating people risks is a key component of the ERM strategy outlined above, so deploy regular anti-fraud awareness training to make sure everyone remains vigilant and informed enough to ward off threats from would-be cybercriminals. While you may have already understood the importance of shielding the accounts of your higher-ups behind wall upon wall of protection, the accounts of your clerks and bookkeepers — or anyone else for that matter — could also be key points of entry for hackers. While it's often easy to detect email phishing scams from their error-ridden content and questionable email addresses, spear phishing is much more sinister and harder to detect, as it often takes the form of a bank or other institution the recipient may be familiar with. Make sure that all personnel are aware of these kinds of threats, and keep everyone on top of the latest software and browser updates to reduce risk.

And while it may be awful to think about, the numbers point to another area that needs to be addressed when improving cybersecurity at your firm: Seventy-seven percent of all data breaches in a year involved an insider to some extent. With such a

high incident rate, it's a potential area of vulnerability that you'd do well to take proactive action to eliminate. Consider limiting the use of outside devices while at work to keep all employees on a secure and centralized system, and work with your IT team to identify and ban applications that could be used with malicious intent. No matter the size of your firm, you are at risk, especially small CPA firms who may not always have a budget for an in-house IT specialist. If you're uncertain about next steps, consult with an IT solutions partner to make sure your business is protected. You never want to suspect your own people of being capable of such an act, but taking the proper precautions on this front is part of doing your due diligence.

Proactivity leads to a thriving future

For CPA firms, cyber attack threats are real and on the rise. Fortunately, there are steps you can take to help mitigate risk and protect the sensitive personal and financial information entrusted to you by your clients. Taking a proactive approach to cybersecurity can make you less susceptible to breaches, lawsuits and customer churn, ultimately helping you maintain your clients — and their trust — to shore up the stability and future success for your firm.

========

Jodi Chavez is Group President of Randstad where she oversees the field organization and provides strategic direction for Randstad Life Sciences, Randstad Professionals and Tatum. With more than 20 years' experience in the staffing industry, Jodi's entrepreneurial drive and strong business acumen have enabled her to consistently increase revenues, grow profits and deliver ROI. Her breadth of expertise spans team building, strategic planning and execution, M&A, branding, social media and multi-generational leadership.

Firm Management • Payroll • Article • Data Breach • data breaches