Accounting for Cybersecurity:

A Guide to Data Security for Accountants and Tax Professionals

Sponsored by:
ADP®
A more human resource.℠

Presented by:
accountingTODAY

Introduction

In an era when cyber attacks occur on a daily basis, financial firms are prime targets. Though mega-banks and retail giants get the spotlight when their customers' financial data is stolen, accountants and their clients are by no means immune. In fact, many cyber thieves prefer to set their sights on smaller firms, believing their security protocols are more lax and more easily compromised.

To learn more about how accountants are dealing with cyber threats, ADP® commissioned SourceMedia/ Accounting Today to survey accounting professionals on this topic.

According to survey findings, many accountants lack a thorough understanding of the issue, even if they recognize that it is an increasing concern. As one account acknowledges, "[Cybersecurity] is a very serious issue which I have not given enough thought to."

Still others believe that cyber intrusions are inevitable. "We expect to be hacked," says one respondent. "We expect to be 'ransomed;' we expect a staffer to have a laptop stolen. We believe we cannot find a way to exempt ourselves from this trouble."

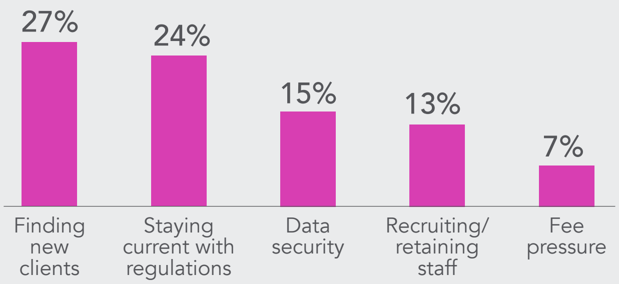
The following white paper lays out the areas of concern for accountants, pinpoints where they are most vulnerable and provides best practices to help avoid falling victim to an attack.

Attractive Targets

It's not hard to see why accountants are vulnerable. First, they possess a trove of sensitive information about their clients—including Social Security numbers, birth dates, addresses and the names of family members. A hacker can easily use this information (and reconstruct passwords and answers to security questions) to gain access into the financial lives of individuals and inflict harm.

Second, as small businesses or sole proprietorships with neither the resources nor expertise to tackle the most sophisticated cyber threats, accountants may not have the latest technology solutions needed to thwart attacks. What's more, accounts often wear so many hats and are stretched so thin that many possess only a cursory understanding of the threats. As a result, data security may not be at the top of their list of priorities. Based on survey results, only 15% of accountants prioritize data security as one of their top three business concerns, below finding new clients and staying current with new regulations (Figure 1).

FIGURE 1. Many Business Issues Vie for Accountants' Attention
Q. Which are your top three overall business concerns?



n = 333
Source: SourceMedia Research, Cybersecurity Study, August 2016

Finally, as accountants increasingly expand beyond tax preparation into wealth management, the problem becomes even more pervasive. These accountants will have not only the standard tax information, but access to bank and brokerage accounts as well. Financial advisers, for their part, routinely report receiving emails from client accounts requesting wire transfers by cyber thieves.

The Big Picture

Just how big of a problem is cybersecurity for accountants? At first glance, it appears that outright data hacks are rare. According to survey results, just 1% of respondents say they have been victims of a data breach. However, there are many other ways that accountants can have data compromised—data hacks are just a small part of the story.

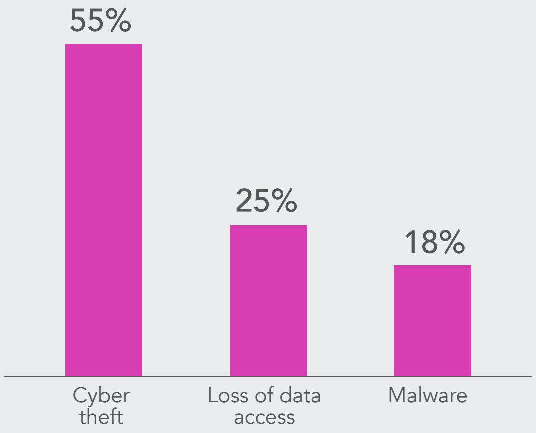
"People are always focused on hacking, when in reality we're talking about the [whole] security of your business," says Roland Cloutier, Staff Vice President and Chief Security Officer with ADP. "[The discussion] should be in the context of business operation protection."

According to survey findings, lapses in data security are not a rare occurrence. In fact, one in 10 accountants report having lost client information in some way such as a lost thumb drive or laptop. Furthermore, nearly 25% of accountants say that they have had a client be the victim of a data breach and about 75% have had clients who were the victims of identify theft.

There are three areas that Cloutier believes accountants must focus on: confidentiality, integrity and availability. Security measures, says Cloutier, must ensure that data remains confidential, in tact and accessible. "You have to think about all the components that your business utilizes from a technology standpoint to ensure that you are protecting each of those areas," he says.

The good news is that accountants appear to be ready to view data security broadly. While more than half of respondents say they are most concerned about data theft, almost a quarter are also worried about loss of data access and malware (Figure 2).

FIGURE 2. Cybersecurity Is more than Hacking
Q. What is your primary concern about data security?



n = 333
Source: SourceMedia Research, Cybersecurity Study, August 2016

A Growing Problem

Cyber threats are picking up. In 2015, the United States was hit with 77,000 attacks, a 10% jump from the year prior, according to the Office of Management and Budget.[1] These threats are likely to continue to grow, even as government agencies allocate additional resources to tackle the problem.

For example, the Internal Revenue Service was hacked in 2015, resulting in data being stolen for more than 700,000 taxpayers. That followed on the heels of a hack in 2013 when more than $5 billion in fraudulent refunds were paid out to cyber thieves.

The cost of cleaning up a cyber crime varies by company, but it can run into the millions for larger firms.[2] Included in the costs are items such as hiring a forensics expert, providing free credit monitoring services to customers affected by the breach and even settling lawsuits.

For example, in September 2015, a St. Louis-based investment advisory firm settled with the Securities and Exchange Commission for storing clients' personally identifiable information on a third-party hosted web server when it was attacked and hackers gained access.

Beyond the direct cost, firms must also allocate staff time to deal with the problem and could suffer long-term reputational damage. "Not only are you risking your brand, you're risking the future of your business," says Cloutier. "You're also risking the consumer who uses your services."

The problem is so pervasive that government agencies are keenly focused on it. The Department of Homeland Security considers cybersecurity crucial in fighting terrorism, as the 2016 hack into the Democratic National Committee's emails demonstrate. Agents acting on behalf of the Russian government are suspected of leaking the emails in an attempt to influence the U.S. election. Further, the National Security Association has formed a task force, NSA21, to stay ahead of cyber threats in the next decade.

The SEC, meanwhile, now includes guidance on cybersecurity for registered investment advisers. A cybersecurity plan is something the SEC is checking for during audits. Specifically, the SEC wants to know what measures firms are taking to prevent a breach and their disaster recovery plans.

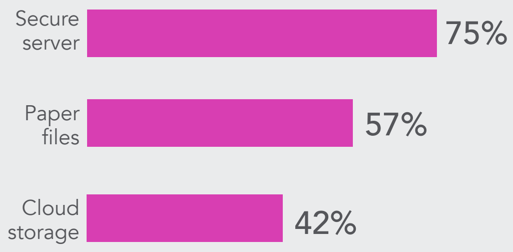
Unfortunately, the current security setups at most accounting firms are lacking, says Cloutier. Accountants leave too many doors open for possible cyber attacks. According to research, many accountants are not using cloud storage, though it is seen as the most secure option for small businesses (Figure 3).

In-house servers, though they provide direct control over data, require both a substantial financial outlay to set up and ongoing maintenance. Having a server necessitates at a minimum a part-time consultant to make sure it is functioning properly.

Paper files have limitations, of course. They are vulnerable to theft and damage in the event of a fire, flood or natural disaster.

FIGURE 3. Accountants not Relying on Secure Data Security Solutions

Q. How do you maintain confidential client information in your practice?



n = 284 (multi-select)
Source: SourceMedia Research, Business Issues Survey, July 2016

[1] Source: Office of Management and Budget, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf

[2] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf

For small firms, cloud storage is both economical and practical. Users only pay for the amount of storage they use. More importantly, cloud storage providers can pass on economies of scale for security. Instead of each business purchasing a security solution, the provider implements one security solution.

"A cloud-based service focuses on the technology while you focus on your clients," says Cloutier. But many accountants express skepticism about cloud storage. "By using paper data it greatly reduces outside risks," one accountant says.

In general, accountants are not that confident in the security solutions they use. More than one-third (37%) say they are either not confident or only somewhat confident in the security measures their firms utilize. These same accountants show even less confidence in the security measure their clients use, with just a quarter saying they are either confident or very confident about the data security measures their clients use.

"My biggest concern is the technology we don't know about and couldn't possibly protect against," one accountant shares.

Take Charge: Best Practices for Data Security

While a sophisticated cyber attack may be in your future, there is no need to make a data breach easy for an attacker to carry out. Think of it this way: There may be break-ins in your neighborhood, but your deadbolt and on-call security system can discourage thieves in a way that your neighbor's wide open door does not.

Practicing good cyber hygiene can prevent up to 83% of cyberattacks, Cloutier says. And you don't have to be an IT expert to employ these strategies. Consider these best practices to cybersecurity.

Mind your business. It sounds simple, but you must understand the entire scope of your business and where technology fits into it. Otherwise, you may not understand potential vulnerabilities.

Make someone accountable. If you're a sole proprietor, you're the person in charge of data security. If you're not up to the task, hire a consultant to oversee this important business function.

Use strong passwords (see sidebar). Take time to create strong passwords that are not easy to guess.

Automate software updates. It's hard to keep abreast of the latest updates and patches, so automate them through your settings menu.

Password Protocol

Data security starts with strong passwords. They are the keys to the kingdom. Ensure that yours are as secure as possible with these steps.

1. **Differentiate.** Use different passwords for each of your accounts. If one password is hacked, it won't compromise everything.

2. **Keep it secret.** Don't let anyone see you enter your passwords, including fellow passengers on a plane.

3. **Log on/log off.** Always log off when you're done with your device.

4. **Watch where you use them.** Avoid entering passwords on shared computers like at an Internet café or library. They may contain malware that steals passwords.

5. **Change it up.** Change your password frequently.

6. **Go for complexity.** Use at least eight characters of lower and upper case letters, numbers and symbols. Avoid your children's or pets' names, your birthday or hometown since those are easy to find out on social media.

7. **Don't write it down.** Instead use a tip sheet that gives you a clue to your password.

8. **Avoid Wifi:** It might be convenient, but many networks are unsecured (as at cafes and airports), allowing hackers to intercept your passwords and data.

Put up a firewall. The routers and modems you use should already have firewalls installed to prevent the malicious intrusions. If not, ask your Internet service provider to install them. The most important thing is to turn them on, and make sure they are functioning properly.

Embrace encryption. Encryption prevents a bad actor from gaining access to your entire network. Even with good credentials, "those individuals won't get access to the full infrastructure," says Cloutier. "They will only get access to what that credential has access to."

Be careful with Wifi: First, make sure you're using wireless encryption. And if you allow outsiders onto your wireless network, create a guest network that doesn't allow access to your internal systems or files.

Educate your clients. Take steps to explain how clients should care for their own data. As one accountant explains, "We have had difficulty getting clients to comply with email security such as sending us confidential data using standard, unencrypted email." Make sure your clients understand the problem—and the risks.

Consider insurance. Cyber insurance can protect your firm from financial ruin if your clients suffer harm due to an attack on your end. In fact, it's a safeguard that more accountants are considering. More than six out of 10 accountants say they carry insurance to cover data breaches.

Conclusion

Although cyberattacks are getting more sophisticated and frequent with each passing year, you and your clients do not need to fall victim to them. Practicing good cyber hygiene can prevent the majority of intrusions by signaling to attackers that you're not an easy target.

To get serious about cybersecurity you must understand the true risks that attacks pose to your business and understand the multiple ways in which your business is vulnerable.

Consider hiring a part-time IT consultant to help you identify gaps in your data security and find solutions that address them. And you may need to rethink your budget priorities to ensure that you're allocating enough resources to purchase the solutions that keep your business safe. Additionally, you will need to spend time training yourself and your staff on the best practices.

These may seem like obstacles at first. But with time and repetition, they are likely to become part of the culture at your practice. Imagine the consequences for not taking action. The very future of your business is at stake.

For more information about ADP and our programs for accounting professionals, contact your ADP representative at 855-408-3751, or visit adp.com/accountant.

Sponsored by:

A more human resource.™

Methodology

In August 2016, SourceMedia Research conducted an online survey on the topic of cybersecurity among 333 accounting and tax professionals, drawn from *Accounting Today*'s opt-in subscriber base.

Supplemental research for Figure 3 is from a SourceMedia Research online study on the topic of business issues conducted among 286 accounting and tax professionals, also drawn from the *Accounting Today* opt-in subscriber base.

About Sourcemedia Research

SourceMedia Research provides full custom B2B research solutions for marketers, agencies and other targeting business sectors, such as accounting, banking, payments, mortgage, insurance, HR/employee benefits and wealth management. SourceMedia Research is a unit of SourceMedia Inc., whose B2B media brands include *Accounting Today, Financial Planning, American Banker, The Bond Buyer* and *Employee Benefit News.*

About ADP

Employers around the world rely on ADP® (Nasdaq: ADP) for cloud-based solutions and services to help manage their most important asset—their people. From human resources and payroll to talent management and benefits administration, ADP brings unmatched depth and expertise in helping clients build a better workforce. A pioneer in Human Capital Management (HCM) and business process outsourcing, ADP serves more than 630,000 clients in more than 100 countries. ADP.com