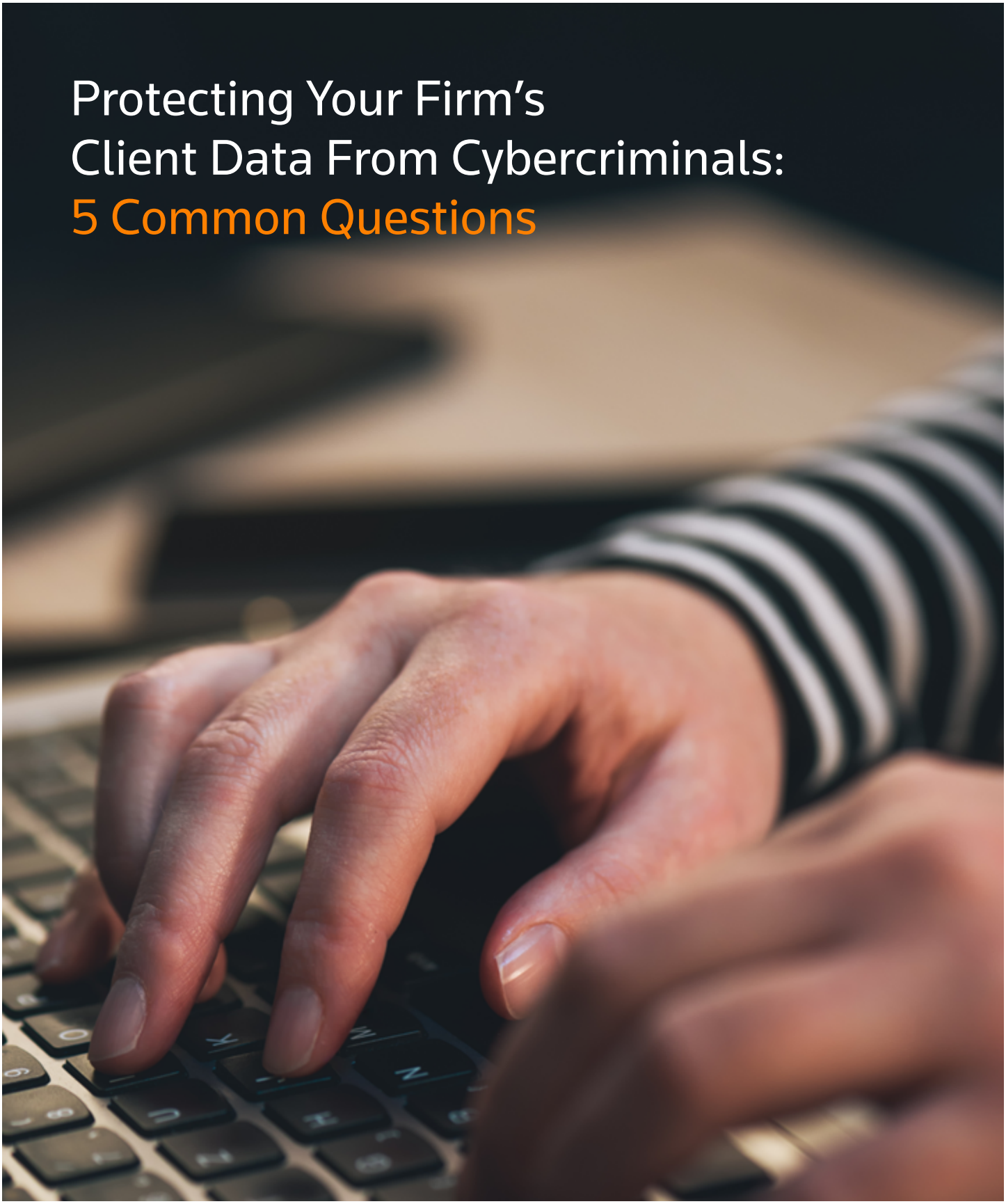
Protecting Your Firm's Client Data From Cybercriminals: 5 Common Questions



tax.tr.com/cs

THOMSON REUTERS®

THE WORLD AS WE NOW KNOW IT

Threats to information come in multiple forms — from malicious (hackers, disgruntled employees) to unintentional (accidental slips of sensitive data by staff). News stories of consumer data breaches are all too frequent, and the tax and accounting profession is not immune to these attacks. In the last two years, criminals have used information obtained from social media to steal return data from taxpayers, and they have also obtained Social Security numbers from outside the IRS and used them to file fraudulent returns electronically.

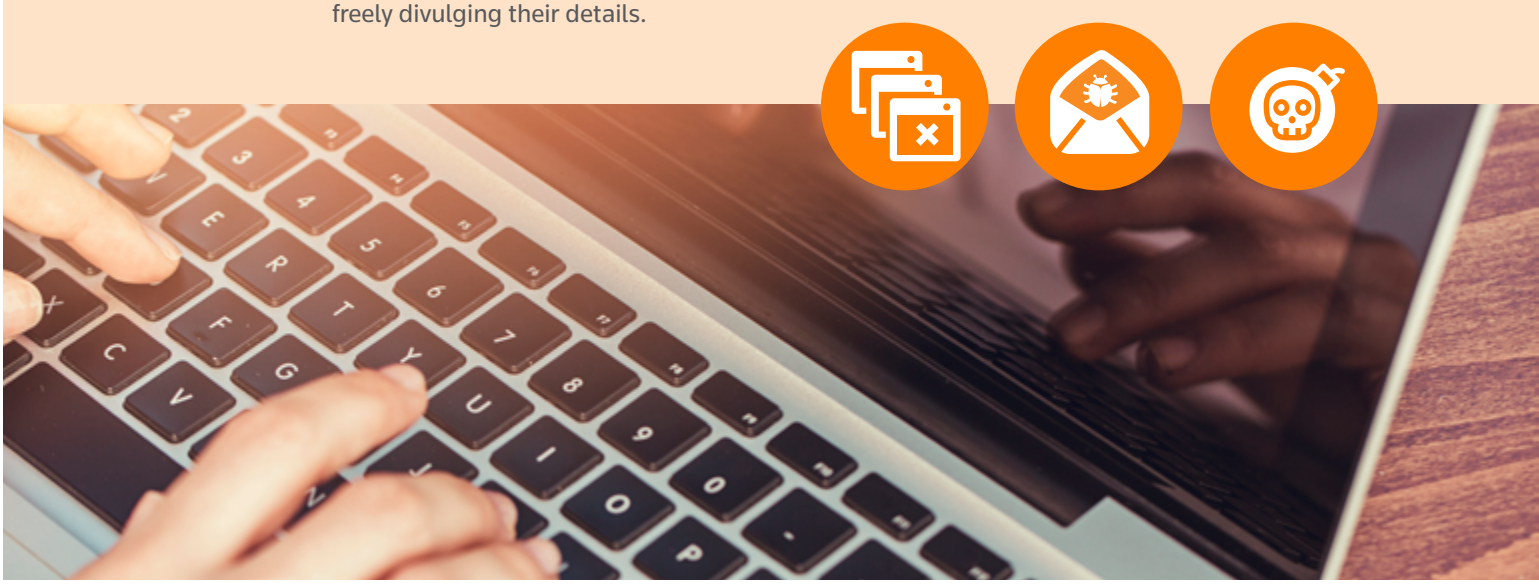
The IRS has worked to stop the proliferation of fraud and reduce the risk to tax preparers and taxpayers — but the agency continues to emphasize that hackers are targeting professional tax preparers in search of client data.

Although cybertheft at large organizations makes headlines, as much as 70-80% of cyberattacks are directed at businesses with fewer than 100 employees. "Small companies are becoming more of a target, because criminals know large firms are devoting more resources to cybersecurity," says Eric McMillen, an information security consultant in Dallas who works with the financial services industry. "A common argument I hear is, 'I'm just a nine-person accounting firm. Why should anyone want to go after me?' Well, you probably have 1,000 or more pieces of client data that a criminal can use."

3 WAYS CRIMINALS CAN STEAL DATA

Cybercrime can be devastating to any firm and its clients. Here are three of the most common methods of data theft.

1. **Phishing** is an attempt by hackers to obtain confidential information from internet users, typically through a web page or an email that masquerades as a trusted source. Believing the request to be legitimate, people can be tricked into freely divulging their details.
2. **Malware** is malicious software that can be delivered to a computer through email attachments and automatically installed on the machine to extract sensitive data, including computer viruses, worms and spyware.
3. **Ransomware** is malware that encrypts and locks people's keyboards or computers to prevent them from accessing their data and leaves instructions — usually for a fee — to regain access.



5 QUESTIONS FIRMS SHOULD BE ASKING ABOUT SECURITY

1. How do I train my employees to be safe?

Employees are the first line of defense in cybersecurity, as they are constantly interacting with clients, colleagues and others on numerous devices — at work, at home and everywhere in between. Educating employees and raising awareness of cybersecurity is crucial.

Sandra Wiley, president of Boomer Consulting Inc., a Kansas-based provider of strategic planning and accounting management services, advises that smaller firms draw up internal policies and also consider outsourcing training.

Best practices for employee safety include:

- **User permissions and restrictions.** Employees should have only as much access to systems as needed to do their specific jobs.
- **A strong password policy.** The IRS advocates that password changes take place every 60 to 90 days and have specific complexity requirements, such as a minimum of eight characters with at least one uppercase letter, one lowercase letter, one number and one special character.
- **Multi-factor authentication.** This extra protection against cybercriminals meets standards that are designed to enhance security by requiring additional criteria to verify your identity, beyond a username and password. For example, the Thomson Reuters Authenticator™ mobile app offers multi-factor authentication.
- **Awareness of scams.** Educate employees about the characteristics of spoof websites (a form of phishing in which a website imitates the website of a legitimate organization) and emails to prevent them from clicking infected phishing or malware links that could send sensitive data to hackers.
- **Cybersecurity hygiene.** Make sure appropriate security is added to all of an employee's digital devices that are used for business: laptops, mobile phones, tablets, etc.
- **Testing and assessing.** Are your employees listening to training and actively implementing best practices? One way to find out is to send an email as a test that imitates a phishing message, for example, before and after training, Wiley says. Then, measure the results.
- **Accountability.** Require employees to sign off on written security policies and procedures at least annually. A lack of ongoing compliance by an employee could possibly lead to termination for putting the firm and its clients at risk.

PASSWORD POWER

According to cloud provider Xcentric, adding two simple tweaks to a standard password can change a hacker's infiltration time from two days to two centuries.

Password	Hacking Time
8 characters, with all lowercase letters	2 days, 6 hours
10 characters, including one capital letter and one asterisk	210 years

SPEAR-PHISHING EXPLAINED

Spear-phishing is the fraudulent practice of sending emails — ostensibly from a known or trusted sender — in order to induce targeted individuals to reveal confidential information. Spear-phishing is a popular method of targeting tax and accounting professionals, and social engineering is the key component of spear-phishing. Here's how it works:

- Bad actors find entities — such as accounting firms, law firms, corporations, etc. — on public websites and glean common information, like names and contact details, off those websites and other online properties like social networks (LinkedIn, Facebook, etc.).
- Next, the bad actors find common outside information, such as product names, logos and URLs of companies that serve those entities.
- This information in turn allows their follow-up communications (typically emails) to appear to come from a legitimate source.

To avoid being a victim, you need to be wary of such attempts and ensure that any communications you receive are, in fact, valid.

2. How do I help my clients prevent identity theft?

Tax professionals need to be aware of the dangers of identity theft — which can occur when a thief files a fraudulent return using another person's tax identification number to obtain a refund — and understand that guarding their confidential tax data is a responsibility shared with their clients.

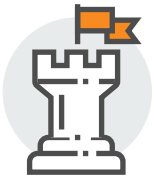
According to the IRS, more than 80% of returns filed in the 2016 tax season will be prepared electronically via tax preparation software. Annual tax return prep presents an opportunity for accounting firms to discuss with clients the need for good data and identity protection to safely deliver information.

The American Institute of CPAs recommends that firms educate their clients about potential cyberspace threats, the firm's security measures and the steps clients can take to ensure their own critical information is protected. "In our profession today, you have to be more than an accountant to your client — you have to be a business advisor," Wiley adds. "This is one of the ways you can do that."

IRS Publication 4524, *Security Awareness for Taxpayers*, includes a checklist that can be shared with clients. Basic safeguards include:

- Using security software that includes a firewall, anti-malware and anti-virus protection that should be set to automatically update against threats
- Using strong passwords
- Recognizing and avoiding phishing emails and other cyberthreats, and reporting them to the IRS
- Filing tax returns early in the season — thieves generally file fraudulent returns early to receive refunds before the actual taxpayers have a chance to file

The IRS also has a series of identity theft videos (youtube.com/irsvideos) that can be valuable to share with clients. The videos include data protection tips such as shredding documents, guarding Social Security numbers and monitoring credit reports.



3. What do I do if my firm has a data breach?

Accounting firms of all sizes should prepare for data breaches. An organized plan will help you respond to an unfortunate incident and manage the aftermath.

In a written policy, you should:

- **Prioritize** who needs to be notified if a breach occurs, starting with the owner/managing partner/administrator at the firm who is responsible for initiating procedures. "Who has the authority to add or turn off services?" asks Trey James, CEO at Xcentric®, a Georgia-based cloud provider exclusive to the accounting industry. Similarly, it's helpful to identify the contact at the cloud service provider — ideally, someone with more authority than the help desk — and determine whether outsourced technology personnel have a role.
- **Define** what needs to be done to contain the data breach, limit loss of data and prevent further breaches from occurring, if possible.
- **Detail** how data should be collected related to the breach, such as date, time, duration, location, how it was discovered, entry or exit points, compromised content and affected personnel and clients.
- **Comply** with federal, state and industry regulations for breach notifications. A fast response is critical. Some states require firms to warn affected clients of the risk of identity theft and fraud within a short time. Go to the IRS website, IRS.gov, for action steps (search "Data Theft Information for Tax Professionals") and contact information for your region's stakeholder liaison.
- **Own up to the responsibility.** "Integrity and professionalism are important," says Wiley of Boomer Consulting. "Contact and provide details to your clients so they can protect themselves." Add a checklist and form letter to your policy identifying people who will communicate with clients and how they will do so.

Also, consider purchasing cyber liability insurance to mitigate risk. Investigating the cause and extent of the breach, paying for credit monitoring services for affected customers, responding to litigation, repairing reputational damage and losing business and employee productivity come at a price. IBM® and Ponemon Institute estimated the cost to an organization for an individual data breach to be $4 million in 2016.

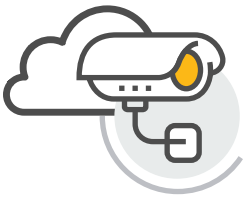
4. How do I help my clients handle identity theft if it happens?

Despite best efforts to protect their data, firms will likely encounter clients who have been victimized by identity theft. If an incident occurs for an individual or business client, take these steps:

- File IRS Form 2848, Power of Attorney and Declaration of Representative, signed by the taxpayer so that you can deal directly with the IRS on a client's behalf.
- Contact the IRS to put a red flag on the account so it can be monitored.
- Complete IRS Form 14039, Identity Theft Affidavit, for the client.
- Provide the client with a six-digit identity protection personal identification number (IP PIN) to file a legitimate return.
- Submit reports to local police and the Federal Trade Commission, close any affected bank or credit card accounts and inform and monitor credit bureaus.
- Remind the client to be patient during what could be a slow process — the IRS averages 278 days to resolve identity theft cases, according to the U.S. Treasury Department.

TAX TIME: WARNING SIGNS OF IDENTITY THEFT

- **Individuals** — If a client's Social Security number has been compromised, the tax return might be rejected with an IRS code indicating the number has already been used — or, if no return was filed, the client might receive a notice from the IRS about a balance due, a refund offset or collection actions.
- **Businesses** — A business taxpayer might receive an IRS notice for a fictitious employee, or an original tax return might be filed for a particular year and accepted as an amended return.



5. Is the cloud safe?

More than half of all firms (56%) use cloud-based software (up 17% from two years ago), according to the 2016 National Management of an Accounting Practice Survey by the American Institute of CPAs. As a business owner, you might be considering replacing your installed server-based software programs and migrating to cloud solutions to better manage your practice and serve your clients.

You may be asking yourself if the cloud is safe. It should come as no surprise that nothing is 100% safe. In a survey of more than 300,000 users across various business segments, CloudPassage®, a cloud security provider, says 9 of 10 organizations are very or moderately concerned about public cloud security.

However, James at Xcentric maintains that the cloud can be more secure than internally installed information technology solutions. In-house software has to be continually patched and monitored by the end user, which isn't always done consistently or correctly. Cloud providers, by contrast, know the success of their businesses hinges on the security of data, and they continuously update their security measures to remain ahead of new threats.

James emphasizes that the greatest security risk to data lies in processes, not technology. In fact, he says humans open most of the doors to hackers. "Sure, technically, there are ways for a hacker to break into the back of a system," he acknowledges. "But the typical security breach comes because someone gave up their credentials unknowingly, such as clicking on an attachment in an email with a malicious link." (See "3 Ways Criminals Can Steal Data" sidebar on page 2.)

So back to the original question: Is the cloud safe? Well, that depends. "The cloud is as safe as the firm decides to make it," says Wiley.

Creating a Safer World Together

Security of personal data is a shared responsibility between you and your technology provider. Together, you can put into place and adhere to security measures to protect client data on the cloud.

Stay up to date with the latest information on security by visiting **tax.tr.com/tag/data-security**.