CPE

CURRICULUM:
Accounting and Auditing; Tax

LEVEL:
Basic

DESIGNED FOR:
CPAs in public practice; tax practitioners

OBJECTIVES:
Discuss and highlight the dangers of poor information security preparation, detail essential responsibilities and regulations, and provide an overview of IRS and FTC guidance on protecting data and addressing breaches

KEY TOPICS:
Information security and cybersecurity overview; professional responsibility to safeguard data privacy; Gramm-Leach-Bliley Act; IRS publications and resources; response to a data breach

PREREQUISITES:
None

ADVANCED PREPARATION:
None

TAKE THE ONLINE CPE QUIZ

Today's CPA offers the self-study exam for readers to earn **one hour of continuing professional education credit.** The questions are based on technical information from the following article. If you score 70 or better, you will receive a certificate verifying you have earned one hour of CPE credit in accordance with the rules of the Texas State Board of Public Accountancy (TSBPA).

Take the CPE quiz online. Go to the News & Publications section of TXCPA's website and select *Today's CPA* Magazine.

The State Board stipulates that the quiz is valid for one year from its publication in *Today's CPA*. Quizzes submitted after this one-year period will not be accepted.

Information Security Plans for Tax Professionals:
A Review of Existing Guidance

BY ERIC GOODEN, PH.D

The Security Summit partners – the IRS, state tax agencies and the tax industry – urge tax professionals to adopt information security plans as cyber incidents rise. With the digitization of accounting, CPAs now shoulder responsibilities for data security and privacy. Cybercriminals increasingly target CPAs, not only for their data but also for access to client accounting systems linked to bank accounts and vendor payments.

This article defines information security, outlines the risks of inadequate planning, reviews key responsibilities and regulations, and summarizes IRS and FTC guidance on safeguarding data and responding to breaches.

INFORMATION SECURITY AND CYBERSECURITY OVERVIEW

Ideally, firms should begin the data security process by understanding the definitions of information security and cybersecurity (Paulsen and Toth, 2016). According to Paulsen and Toth (2016), information security is the protection of digital information and related systems from unauthorized alteration, delay, destruction, use, access, disclosure, or disruption to provide confidentiality, integrity and availability. It encompasses people, processes and technologies.

According to Paulsen and Toth, cybersecurity is key to information security and means protecting electronic devices and electronically stored information. It is formally defined as preventing damage to, protecting and restoring electronic records, software and related hardware to maintain integrity, confidentiality, availability, verification, and nonrepudiation.

An information security incident can be devastating for CPA firms. The greatest risk is data theft, where cybercriminals steal sensitive client financial and personal information to commit fraud. For firms, this leads to infrastructure damage, litigation, productivity loss, higher costs, and reputational harm. For clients, breaches open the door to fraud schemes such as manipulated records, fake vendors, redirected payments, or unauthorized transactions.

Cybercriminals increasingly target small businesses, which often lack strong governance and security, making them easy prey. These clients may hold valuable assets or data, and compromised systems can be used to attack others. CPA firms must stay vigilant, as a weakness at one client can endanger many.

To combat breaches, the IRS requires written information security plans (WISPs). A breach may signal noncompliance, which also violates state and federal privacy laws and can result in fines or sanctions. CPA firms that fail to comply with data privacy laws face steep penalties. Likewise, the AICPA Code of Professional Conduct requires adherence to legal standards and violations can lead to disciplinary action from state boards or AICPA.

PROFESSIONAL RESPONSIBILITIES

Data privacy is not a new concept in the accounting profession and CPAs have always been required to take reasonable steps to safeguard data privacy. For example, the "Confidential Client Information Rule" is a well-established professional duty in the AICPA Code (AICPA, ET §1.700). Similarly, the Code has always required CPAs to act in their client's best interest and uphold the public trust.

What is new concerning information security, specifically for tax professionals, is that AICPA has revised its Statements on Standards for Tax Services (SSTSs), effective January 1, 2024, to address data protection, adding Section 1.3, which uses standards to describe reasonable efforts to safeguard taxpayer data rather than

setting strict rules. This standard broadly considers firm differences and constant technological changes, laws and threats. CPAs applying this standard should consider laws, data storage methods, digital tools, and third-party providers.

Firms must review privacy policies based on technology, services and size—ensuring even sole practitioners use protections like antivirus software, VPNs, secure programs, and strong passwords. They should also provide

employee training, set data retention policies and use encryption for personal information.

KEY REGULATORS AND REGULATORY REQUIREMENTS

The Gramm-Leach-Bliley Act (Safeguards Rule) applies to all tax return preparation firms regardless of size and requires a WISP describing how the business protects consumers' nonpublic personal information. The IRS and FTC have increased their focus on this rule.

Related CPE:

- IRS Cybersecurity Checklist
- Mastering The Three Pillars of Cybersecurity: Exploring the Technology Pillar
- Surgent's Foundations of Cybersecurity for Financial Professionals

Federal law, enforced by the FTC, mandates that all professional tax preparers utilize a WISP. In addition to increased data security, the Security Summit, through the Tax Professional Working Group, notes that a WISP can be helpful in other disruptive events like fire, flood or theft. Accordingly, creating a WISP is critical to running a successful tax preparation business.

The scope and complexity of a security plan should be appropriate to the company's size, activities, and the sensitivity of the customer data in question. Thus, there is no one-size-fits-all solution to developing a good WISP. Instead, a good WISP should focus on key factors, including prevention, detection and oversight of system failures, system hardware and software protection, and employee training and oversight. The FTC's Data Breach Response Guide PDF is a valuable resource and is discussed below.

IRS PUBLICATIONS AND RESOURCES

The IRS provides several publications and resources designed to assist professionals in understanding data security issues and developing an effective response strategy. For example, IRS Publication 5293 focuses on critical aspects of data security concerning protecting clients and the tax professional's business from the increasing threat of data theft. This publication outlines several key areas where tax professionals can focus to establish and maintain robust security measures for safeguarding sensitive taxpayer data.

Similarly, IRS Publication 4557 provides guidelines on handling and protecting taxpayer information. Publication 4557 also outlines administrative, technical and physical security guidelines. The key points of Publication 5293 and 4557 are summarized below. Please see Figure 1 for data privacy regulations when operating across jurisdictions.

IRS Publication 5293, *Protect Your Clients; Protect Yourself: Data Security Resource Guide for Tax Professionals*, and IRS Publication 4557, *Safeguarding Taxpayer Data*, are available at IRS.gov. Key points from both documents are noted below.

Implementing basic security steps involves the execution of several key control activities concerning data security, including:

- Recognizing phishing attempts,
- Creating a data security plan,
- Reviewing internal controls,
- Regularly updating anti-malware software,
- Using strong passwords with multi-factor authentication and encrypting sensitive data,
- Backing up data securely,
- Carefully reviewing return information before filing,
- Properly disposing of old hardware,
- Limiting data access to taxpayer information,
- Monitoring electronic filing identification numbers (EFIN) and preparer tax identification numbers (PTIN) accounts,
- Staying informed through IRS resources, educating clients, and reviewing FTC security tips and guidelines.

In addition to control activities, an essential dimension of any system of internal control environment is the monitoring process. Monitoring controls ensure systems function properly while identifying areas for improvement. Publication 4557 advises firms to detect and manage failures by monitoring threats, updating security controls, using intrusion detection, tracking data transfers, and preparing breach responses. Firms should also monitor EFIN/PTIN accounts, follow IRS updates, maintain audit trails, and educate clients on emerging risks.

Security software is a critical component of data security and the IRS guidance notes that it is vital to download security software only from official vendor sites. Software utilization processes include installing and regularly updating firewall software, using drive encryption, anti-virus and spyware software, and ensuring that security software and internet browsers regularly receive automatic updates.

It is important to create strong passwords. Strong password creation includes requirements regarding complexity, including limita-

tions on repeated characters. For example, requiring complex character combinations (symbols, letters and numbers). Password complexity may also include the implementation of minimum character requirements. Older guidelines suggested eight characters. Security experts now recommend a minimum of 12 characters or 16 characters for system administrators.

Concerning the creation of strong passwords, IRS Publication 5293 advises tax professionals to use strong, confidential passwords – avoiding personal details, changing defaults, not reusing old ones, and considering password managers. It also recommends multi-factor authentication for all critical functions, especially those involving client data.

Protecting client data starts with locking down both wireless networks and internal systems. On the wireless side: change default router passwords, use a non-identifying SSID, limit network range, enable WPA-3 encryption, avoid WEP and public Wi-Fi, and require VPNs with multi-factor authentication for remote access.

Figure 1. Data Privacy Regulations for CPAs Operating Across Jurisdictions

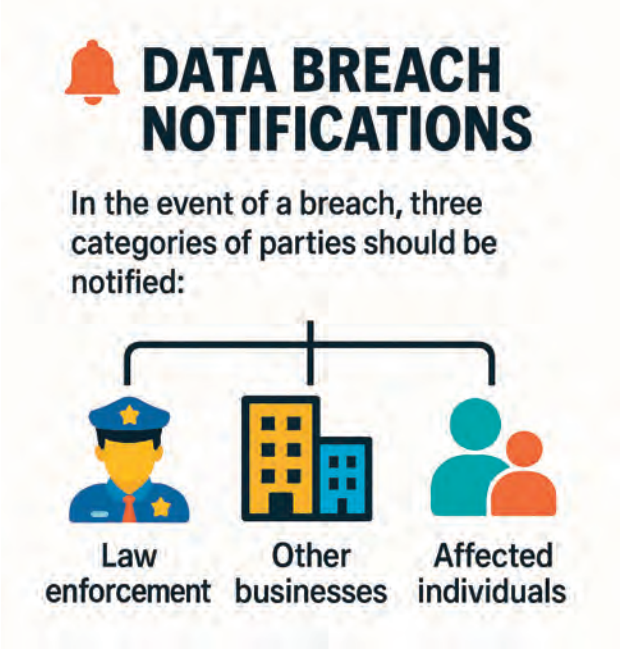
International Regulations:
- GDPR (European Union)
- PDPA (Argentina)

U.S. State Regulations:
- CCPA (California)
- CPA (Colorado)
- TDPA (Connecticut)
- VCDPA (Virginia)

Key Considerations:
- CPAs must navigate complex data privacy laws.
- Regulations mandate data protection obligations.
- Applies to handling personal data both internationally and domestically.

For information systems, know where sensitive data resides and protect it with strong passwords, encryption and secure backups. Transmit files only through protected channels like SSL or SFTP. These steps build critical layers of defense, reducing risk and strengthening client trust.

Protecting stored client data includes backing up encrypted data to secure external sources or the cloud (encrypting before upload), using drive encryption, avoiding public computers for client data, limiting software installations, maintaining a device and software inventory, limiting internet access for data storage devices, and securely disposing of old devices and client information. Publication 4557 strongly recommends using multi-factor authentication for accessing sensitive information.



Professional vigilance suggests being aware of the signs of data theft, such as rejected returns, clients receiving unexpected IRS communications or refunds, unauthorized account access, discrepancies in filed returns, and unusual computer activity. Monitoring electronic filing identification numbers (EFIN) and Preparer Tax Identification Number (PTIN) accounts weekly is crucial. Education on phishing and spear phishing is also vital.

When a data breach occurs, Publication 4557 advises tax professionals to act quickly. Steps include:
- Reporting breaches to the IRS, law enforcement and state agencies,
- Contacting security experts and insurers,
- Reviewing FTC guidance,
- Identifying the cause,
- Developing a continuity plan, and
- Maintaining full backups

FTC SAFEGUARDS RULE

Complying with the FTC Safeguards Rule is required under the Gramm-Leach-Bliley Act. Tax preparers must maintain a WISP suited to their size and complexity. A WISP should designate a responsible individual and cover employee training, multi-factor authentication, risk assessments, system safeguards, service provider oversight, and ongoing monitoring and remediation of vulnerabilities.

Even strong WISPs can fail, so CPA firms must know how to respond when breaches occur. The FTC's *Data Breach Response: A Guide for Business* outlines critical steps firms should follow in managing an incident.

RESPONDING TO A DATA BREACH

Securing operations is the first step in the response to a data breach. CPAs must be prepared to treat the operational areas impacted by a data breach like a crime scene investigator. For example, secure physical areas by locking access and updating codes. Protect affected systems by taking equipment offline (without shutting it down), monitoring entry points and updating user credentials. Finally, address the vulnerabilities that caused the breach to prevent recurrence.

After a data breach has occurred, the response team should be mobilized to prevent additional data loss. A data breach response team should be designated before a breach incident. The team should include individuals with the requisite expertise in areas affected by the data breach, including experts in computer forensics, legal, information technology, and human resources. Given the structure of many CPA firms, this may require outside expertise, particularly in the areas of digital forensics, information technology, and legal. Please see Figure 2 for mobilization considerations.

Another important step is to fix vulnerabilities. Fixing vulnerabilities is simply the process of identifying and remediating the weaknesses in the information system that allowed the breach to occur.

A comprehensive communications plan should be in place that addresses all potential stakeholders (employees, customers, investors, business partners, etc.) and should avoid misleading statements or provisions that may withhold key details that could help consumers protect themselves. Additionally, the plan should avoid publicly sharing information that might put consumers at further risk. The plan should also anticipate questions and provide clear, plain-language answers on your website.

NOTIFICATIONS

In the event of a breach, three categories of parties should be notified: law enforcement, other businesses and affected individuals. In addition to the parties noted above, CPAs should explicitly consider the legal requirements regarding data breach notification under applicable state and federal laws.

In particular, law enforcement, such as the local police, FBI, Secret Service (for electronic breaches), or the U.S. Postal Inspection Service (for mail theft), should be contacted immediately. If electronic personal health records are involved, check if the Health Breach Notification Rule applies and notify the FTC and possibly the media. If the HIPAA Breach Notification Rule applies, inform the Secretary of Department of Health and Human Services (HHS) and perhaps the press.

Concerning the timing of notifications to additional parties, such as the media, CPAs should consult law enforcement to avoid unduly compromising the investigation.

CPAs should notify affected businesses, especially if account access information was stolen but is maintained by another institution or if you collected or stored personal information on their behalf. If cybercriminals have stolen SSNs, contact the major credit bureaus for guidance and advise them if you recommend fraud alerts or credit freezes.

CPAs should also notify individuals promptly so they can take steps to protect themselves. The notification should be made in light of thoughtful consideration of all the facts and circumstances of the specific incident. Tax professionals should explicitly consider factors such as the likelihood of misuse of the compromised data, the regulatory requirements of applicable privacy laws, the nature of the breach, potential damages, and the compromised information type.

Figure 2. Mobilization Considerations for a Data Breach Response

1. Legal and Expert Consultation
   - Consult Legal Counsel: Especially with privacy/data security expertise.
   - Assemble Response Team: Include digital forensic experts.
2. Digital Forensics
   - Identify Breach Source
   - Collect Evidence: Forensic imaging, analysis, remediation steps
   - Consider External Experts: If breach is complex or resources are limited
3. Immediate Actions
   - Remove Exposed Data: From your site and cached search results
   - Search and Request Removal: Of leaked data from other websites
4. Investigation and Documentation
   - Interview Witnesses
   - Preserve Evidence
   - Document Findings
5. Service Provider Review
   - Assess Access and Security
   - Confirm Fixes to Vulnerabilities
6. Network and Data Review
   - Check Network Segmentation
   - Analyze Encryption, Backups, Logs
   - Restrict Data Access
   - Verify Compromised Data and Affected Individuals
7. Remediation
   - Implement Forensic Recommendations Promptly

PROTECTING CLIENT DATA: A PROFESSIONAL AND LEGAL RESPONSIBILITY

Data security is a critical issue for CPA firms in recent years due to changes in practice, technological developments, threats from cybercriminals, and new legislation. Data security is particularly vital for tax professionals, given their access to sensitive personal information.

While complete data privacy cannot be guaranteed, the courts expect CPAs to take reasonable steps in their business practices to ensure data privacy for their clients. Key expectations for CPAs include staying updated on regulations and threats, maintaining a WISP, developing internal data protection policies, and keeping clients informed.

The article also provides helpful summaries of IRS and FTC guidance regarding data security plans and steps to take in the event of a data breach. Addressing the matters noted in this article should help tax professionals ensure compliance with applicable regulatory/professional standards concerning data privacy, which in turn may significantly limit their legal liability and associated costs.

References

AICPA. 2023. *Statements on Standards for Tax Services*. Issued by the Tax Executive Committee. Effective Date: January 1, 2024, Accessed January 7, 2025, Available at: https://www.aicpa-cima.com/resources/download/revised-statements-on-standards-for-tax-services-no-1-4-1-1-2024

AICPA Code of Professional Conduct, ET §1.700, *Confidential Client Information Rule*.

Controlaltprotect. 2024. *Another Reason Why Cybercriminals Attack CPAs*, Accessed Controlaltprotect website, Updated: November 30, 2024, Accessed February 3, 2025, Available at: https://www.controlaltprotect.com/another-reason-why-cybercriminals-attack-cpas/

Federal Trade Commission. 2021. *Data Breach Response: A Guide for Business*. Updated: April 3, 2024, Accessed January 7, 2025, Available at: https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

IRS. 2018. *Protect Your Clients; Protect Yourself: Data Security Resource Guide for Tax Professionals*. Publication 5293, Accessed January 7, 2025, Available at: https://www.irs.gov/pub/irs-pdf/p5293.pdf

IRS. 2024. *Safeguarding Taxpayer Data: A Guide for Your Business*. Publication 4557, Accessed January 7, 2025, Available at: https://www.irs.gov/pub/irs-pdf/p4557.pdf

Paulsen, Celia, and Patricia Toth. 2016. "Small Business Information Security: The Fundamentals." NIST Interagency Report 7621 Revision 1, National Institute of Standards and Technology, Accessed January 7, 2025, Available at: https://doi.org/10.6028/NIST.IR.7621r1

ERIC GOODEN, PH.D., is an Associate Professor at Boise State University. Contact him at ericgooden@boisestate.edu.