Cybersecurity for Tax Preparers

Julie R. Shank
304-230-1804
jshank@bowlesrice.com

Facts

- Average cost of a small business data breach is $2.5 million.
- There is a hack attack every 39 seconds
- Research data suggests that cybercrime will cost businesses over $2 trillion total in 2019.
- 95% of cybersecurity breaches are due to human error

What do hackers want?

- Your client's data!
  - Types of data
- Sell it on the Dark or Deep Web

How does data get into the wrong hands?

- Stolen computers, flash drives
- Employee takes client info
- Cybercriminals hacking into your system

Cybercriminal tactics

- Ransomware
- Malware
- Phishing
- Spear-phishing
  - Personalized Message
  - Account take over
  - Computer take over
  - Report to phishing@irs.gov

How to deal with phishing e-mails

- Don’t reply
- If suspicious, contact sender by alternative means (phone, etc.)
- Educate workforce
- Process for reporting phishing e-mails

Avoid ransomware

- Don’t click on unknown links
- Anti-virus software
- Back up information
- Educate employees
- Generally, be aware

What Is Required For Financial Institutions?

- The Federal Trade Commission (FTC) requires all tax preparers to create and enact security plans.
- All financial institutions — including CPA firms — must safeguard sensitive data under the Gramm-Leach-Bliley (GLB) Act.
- All financial institutions must develop a written information security plan that describes how they're prepared to safeguard client information.
- The FTC-required information security plan must be appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles.

What Must Be In Your Security Plan

- According to the FTC, each company, as part of its plan, must:
  - designate one or more employees to coordinate its information security program;
  - identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;
  - design and implement a safeguards program and regularly monitor and test it;
  - select service providers that can maintain appropriate safeguards, make sure the contract requires them to maintain safeguards and oversee their handling of customer information; and
  - evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.
- The FTC says the requirements are designed to be flexible so that companies can implement safeguards appropriate to their own circumstances. The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operations.

“Taxes Security Together Checklist”

- Put out by the IRS urging tax professionals to review basic security measures.
- The "Taxes-Security-Together" Checklist highlights key security features:
- Deploy the “Security Six” measures:
  - Activate anti-virus software.
  - Use a firewall.
  - Opt for two-factor authentication when it’s offered.
  - Use backup software/services.
  - Use Drive encryption.
  - Create and secure Virtual Private Networks.

“Taxes Security Together Checklist” (cont.)

- Create a data security plan:
  - Federal law requires all “professional tax preparers” to create and maintain an information security plan for client data.
  - The security plan requirement is flexible enough to fit any size of tax preparation firm, from small to large.
  - Tax professionals are asked to focus on key risk areas such as employee management and training; information systems; and detecting and managing system failures.

“Taxes Security Together Checklist” cont.

- Educate yourself and be alert to key email scams, a frequent risk area involving:
  - Learn about spear phishing emails.
  - Beware ransomware.
- Recognize the signs of client data theft:
  - Clients receive IRS letters about suspicious tax returns in their name.
  - More tax returns filed with a practitioner’s Electronic Filing Identification Number than submitted.
  - Clients receive tax transcripts they did not request.
- Create a data theft recovery plan including:
  - Contact the local IRS Stakeholder Liaison immediately.
    See https://www.irs.gov/businesses/small-businesses-self- employed/stakeholder-liaison-local-contacts
  - Assist the IRS in protecting clients’ accounts.
  - Contract with a cybersecurity expert to help prevent and stop thefts.
- IRS Publication 4557, Safeguarding Taxpayer Data (PDF), details critical security measures that all tax professionals should enact.

Additional Data Protection Provisions May Apply

- IRS Publication 3112 - IRS e-File Application and Participation, states: Safeguarding of IRS e-file from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers. Providers must be diligent in recognizing fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request information and documents related to returns with potential fraud or abuse.
- IRC, Section 7216 - This IRS code provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses information furnished to them in connection with the preparation of an income tax return.
- IRC, Section 6713 - This code provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.
- IRS Revenue Procedure 2007-40 - This legal guidance requires authorized IRS e-file providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations put into effect by the FTC, as well as violations of non-disclosure rules addressed in IRC sections 6713 and 7216, are considered violations of Revenue Procedure 2007-40. These violations are subject to penalties or sanctions specified in the Revenue Procedure.

QUESTIONS?