Introduction

Tax professionals are prime targets for identity thieves. Why? Your clients' information — bank and investment accounts, Social Security numbers, health insurance records, and more — can be a virtual goldmine in the wrong hands. That's why securing it against unauthorized access is critical to protect your clients and your business.

Agenda

- Current Trends in Cyber Risks
- Security Challenges During Pandemic
- How to Minimize Risks with Planning
- Laws Applicable
- Practicing Cyber Hygiene
Current Trends in Cyber Threats
The average time to identify and contain a breach is 280 days.
(2020 Ponemon Report)

Average Cost of a Data Breach in 2020
- $3.86 million
  - Having a remote workforce was found to increase the average total cost of a data breach by nearly $137,000 from 2019, for an adjusted average total cost of $4 million.
(2020 Ponemon Report)

Current trends - What is the threat landscape?
- What are the threats to a tax preparer’s operations, infrastructure and/or data?
  - Unintended disclosures by employees; Employee Error
  - Hacking/Malware/Ransomware
  - Insider Wrong-Doing
  - Zero Day Vulnerabilities
  - Physical Loss
  - Portable Device/Removable Media
Current trends – threat landscape con’t

- Technology Intrusions
- Phishing/Spear-Phishing Scheme
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors – Poor Security
  Protocols/Standards

A Current Perspective

Over the centuries, our societies have persevered through global pandemics similar to the coronavirus (and worse).

What’s different about this crisis is its cybersecurity impact.

Sudden work-from-home business models, increased exposure to unmitigated digital risk, and opportunistic attackers are exacerbating an already difficult situation.

Ransomware

- Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid (usually in bitcoin).
- Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.
Recent Ransomware Attacks

- The line between ransomware attacks and data breaches continues to blur in 2020, with a number of prolific ransomware operators – including Maze, Sodinokibi, DoppelPaymer, Nefilim, Clop, and Sekhmet – creating their own websites where they publish the stolen data of non-paying victims.

Recent Attacks – Maze ransomware

- The Maze ransomware ring has taken extortion to new heights by publicly posting breached data on the Internet—and threatening full dumps of stolen data if the ring’s “customers” don’t pay for their files to be unencrypted.

MAZE Ransomware

- FBI alert announced regarding Maze ransomware attacks & that attackers were impersonating government agencies
- French government recently published a Maze alert
- Maze uses multiple methods for intrusion
- Maze actors encrypt files and then threaten to release confidential and sensitive files in an effort to secure the ransom payment
- Law firms, medical providers, municipalities, businesses targeted in recent Maze attacks
Examples of Public Shaming

The criminals behind the Maze ransomware launched a “public shaming site” at mazenews.top, which contains a rapidly expanding list of victimized organizations that refuse to cough up the ransom. The extra details include the breach date and the total amount of collected data. Some entries contain proofs of the attack in the form of ZIP archives with a portion of illegally withdrawn information.

How do Ransomware Attacks Occur?

- Phishing
  - A malicious “spam-like” message sent in large batches to broad audience

- Zero-Day Vulnerabilities
  - Threats related to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it means an official patch or update to fix the issue hasn’t been released, making the vulnerability easy for hackers to exploit.

What Happens During a Ransomware Attack?

- Demands ransom to remove the restrictions;
- Some forms systematically encrypt files on the system’s hard drive;
- Difficult or impossible to decrypt without paying the ransom for the decryption key, some may simply lock the system and display messages to coax the user into paying;
- Most ransomware enters the system through attachments to an email message or can be as a result of a zero-day vulnerability;
- For consideration:
  - Don’t click on unknown links;
  - Keep your anti-virus software up-to-date;
  - Back up all sensitive information;
  - Employee education.
FBI Urges Vigilance During COVID-19 Pandemic

- April 13, 2020
  - FBI warns of rise in scams involving cryptocurrency related to COVID-19 pandemic:
    - Blackmail attempts;
    - COVID-19-themed phishing messages or malicious applications;
    - Work-from-home scams;
    - Paying for non-existent treatments or equipment;
    - Investment scams.

Telework Cyber Risks

- Understand Fear & Distraction
- Clicking on links and attachments
- Unsecure Wi-Fi connections
  - Must use a secure Wi-Fi and VPN connection
  - Passwords for routers and Wi-Fi
- Risk of others in household using the work laptop or mobile device
  - Use passwords for remote logins
  - Use multi-factor authentication
- So many mobile devices – risk of loss, theft – especially for unencrypted devices
  - Violations of confidentiality – who’s listening?
  - Is the data properly and regularly backed up?

Security Challenges Related to COVID-19 Pandemic

- Telework – more exposed systems and data;
- Unpatched and out-of-date systems, and IoT (Internet of Things) devices at home enabled and listening (e.g., home security cameras, Alexa, etc.)
- Increased use of (insecure) personal mobile devices;
- Unprotected wireless networks used to join VPNs and remotely access corporate networks and sensitive data;
- Increase in social engineering & phishing attempts using COVID-19-themed phishing messages to conduct ransomware attacks or implant malware;
- Large-scale stimulus fraud and stimulus-themed spear-phishing campaigns;
- Violations of confidentiality – who’s listening? IoT concerns;
- Is your data properly and regularly backed up?
- Increased collection of health information from employees (e.g., temperature checks, answers to screening questions, contact tracing apps).
IoT Devices—They are Listening

- IoT devices listen for the "wake" word and then the device will begin recording – What can you do to protect private/confidential information while working from home?
  - Unplug the device during the work day;
  - Turn the microphone (and camera) on the device off during the work day;
  - Manage and delete audio recordings using the Alexa app;
  - Make sure your home security cameras don’t point at your screen.

Tips for Remote Workers

- Proper Tools, Apps, and Equipment
  - IT should make sure VPN can handle additional workload, especially for legacy systems and applications that are not cloud-based.
  - Check subscriptions to common apps to make sure they meet the enterprise privacy and security requirements. For example, do you have the licenses on cloud services – platforms, software – to address regulatory privacy and security requirements for additional workers who would normally only work in the controlled environment.
  - Several tech companies are making their tools available, such as Microsoft, Google, LogMeIn, Cisco Webex, Zoom.
  - Check the privacy settings for whichever tools you use, to avoid the over-collection of personal data of your employees, customers, prospects, and other business contacts.
**Incident Notification and Security Concerns**
- All employees should have the contact name, number, and email for security concerns in their phones and/or location other than their standard work device.
- Remind employees about confidential data handling protocols, and remind regularly of security reminders for phishing, etc.
- Remind employees on privacy and security measures and incident reporting requirements.
- Also, conduct a remote mock incident response.
- SANS remote work toolkit

**Confidential Data Awareness**
- Remind employees about confidential data, including both personal data and business data, such as trade secrets.
- Make sure documents are not downloaded unless necessary and minimize transmission.
- If confidential data must be emailed or shared, use encryption.

**What can you do to protect your business?**
Determine where your high-risk data is, where it is going, and the overall data flow so that you know how to protect it (and who to protect it from)
Identifying and Protecting High-Risk Data

- Social Security number
- Driver’s license number or state-issue identification card number
- Passport number
- TIN/EIN
- Alien registration number or tribal identification number
- Financial account number, credit card number, or debit card number with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account, or deposit or savings account number

Identifying and Protecting High-Risk Data (cont’d)

- Medical or health insurance information
- Username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account
- Biometrics

Enterprise-Wide Privacy + Security Program

- Conduct a security risk assessment
- Protect your data
  - Paper records
  - Stored in locked areas
  - Retain only as necessary
  - Electronic records
  - Segregate highly sensitive data
  - Access controls & user authentication
- Data retention and destruction program
### Enterprise-Wide Privacy + Security Program (cont’d)

- Policies and procedures as legally required to address
  - Privacy
  - Security
- Technology to secure it
  - Encryption
  - Firewalls
- Educate users and employees
- Designate Privacy & Security Team
- Designate Incident Response Team

### Vendor Management

- Map all vendors who have access to personal information
  - Follow the data
- Put vendor confidentiality agreements in place with each
  - Payroll/HR
  - Benefits/insurance
  - Website hosting provider
  - Cloud service provider
  - IT service providers
  - CPAs/Legal

### Education & Training

- Conduct employee and user education and training at least yearly on data privacy and security, risks and how to protect your organization
- Keep records of the training
- Each employee/user should sign an acknowledgement form after attending the training
Understand the Laws that Apply to Your Business

- IRC Regulations
- State Data Breach Notification Law(s)
- State Laws Applicable to Tax Preparers
  - Virginia

Privacy & Security Policies, Procedures and Standards

- Have a data security plan in place (IRS tax tip 2019-174)
- Acceptable Use Procedure;
- Social Media Standards and Guidelines;
- Bring Your Own Device (BYOD) Program;
- E-mail Procedure;
- Data Retention Program and Retention Schedule;
- HIPAA Compliance
  - If self-funded health plan.
  - Telework Security Considerations.

Develop an Incident Response Plan

- Create an Incident Response and Breach Notification Plan BEFORE an incident occurs:
  - To be effective, the incident response plan and breach notification process must be part of a comprehensive information security plan:
    - Risk assessment (organization’s most critical assets & data flow)
    - Trigger events (how to identify/verify intrusion)
    - Mitigation plan (minimizing damages)
  - Identify State and Federal Laws and Requirements
  - Breach Notification Laws Across the Country
  - 50 State Breach Notification Laws
  - Communications/Media Team/Vendors in Place
- For larger businesses: assemble an incident response team and assign overall responsibility for enterprise-wide information privacy & security oversight (appoint a data privacy officer and a data security officer).
BYOD Program

- Goal: To assist employees in being responsive and accessible and utilize their personal mobile device(s) for business purposes as well as for their convenience
  - BYOD programs allow the use of personal mobile devices by employees who are authorized to participate in the BYOD program.
  - Employees must agree to and follow the Company’s BYOD policies and procedures so that they clearly understand their rights and obligations when using their personal device(s) for Company business purposes.

BYOD Checklist

- Make sure that each mobile device is registered with the Information Technology (“IT”) Department;
- Require employees to sign a statement acknowledging the Company’s BYOD program;
- Reserve the right to terminate BYOD user authorization at any time and make clear that violations of the BYOD program may result in disciplinary action up to and including termination;
- Provide employees with information concerning how to access all policies and procedures related to the BYOD program;
- Establish that users must set a password for access to the mobile device and require multi-factor authentication for access to Company’s programs or applications.

National Institutes for Standards & Technology (NIST) Telework Recommendations

- Developing and enforcing a telework security policy, such as having tiered levels of remote access;
- Requiring multi-factor authentication for enterprise access;
- Using validated encryption technologies to protect communications and data stored on the client devices;
- Ensuring that remote access servers are secured effectively and kept fully patched; and
- Securing all types of telework client devices – including desktop and laptop computers, smartphones, and tablets – against common threats.
Cyber Hygiene Best Practices

Laptops, USBs, portable hard drives, and smartphones are high risk if they contain personal information or other confidential business information:
- Stolen unencrypted mobile devices still an issue every day;
- Lost laptops and USB drives;
- Connecting to an unsecure Wi-Fi network.

Never give someone remote access to your device, even if they say they're calling from IT.

If a mobile device contains personal information that information is accessed, used, or disclosed by an unauthorized individual you may be required to notify under state law.

Risks with using USB drives:
- Cyber criminals starting to write viruses and worms that specifically target USBs;
- So small they're easy to lose;
- If a lost or stolen USB drive contains sensitive personal information that's not encrypted or secured, it could be a reportable data breach.

Be Aware of Risks from Mobile Devices and Removable Media

- Laptops, USBs, portable hard drives, and smartphones are high risk if they contain personal information or other confidential business information:
  - Stolen unencrypted mobile devices still an issue every day;
  - Lost laptops and USB drives;
  - Connecting to an unsecure Wi-Fi network.
- Never give someone remote access to your device, even if they say they're calling from IT.
- If a mobile device contains personal information and that information is accessed, used, or disclosed by an unauthorized individual you may be required to notify under state law.
- Risks with using USB drives:
  - Cyber criminals starting to write viruses and worms that specifically target USBs;
  - So small they're easy to lose;
  - If a lost or stolen USB drive contains sensitive personal information that's not encrypted or secured, it could be a reportable data breach.

Mobile Devices

How to manage mobile devices:
- Decide whether mobile devices will be used to access, receive, transmit or store personal information and other confidential business information or used as part of an internal network or system;
- Consider how mobile devices affect the risk;
- Establish a BYOD Program: Identify mobile device risk management strategy;
- Educate employees about mobile device privacy and security awareness and best practices.

How can you protect and secure data when using a mobile device?
- Use a complex password/passphrase or other user authentication (multi-factor authentication);
- Install and enable encryption;
- Install and activate remote wiping and/or remote disabling;
- Disable and do not install or use file sharing applications;
- Install and enable a firewall.
Mobile Devices (cont’d)

- PRIVACY SETTINGS
  - Location, microphone

Transportation of Data

- Use a chain of custody log: Track data, times, and dates of transfers, names and signatures of individuals releasing the information, and include a general description of the information being released.
- Protect Paper Records: Use non-transparent envelopes and boxes; encrypt electronic records.
- Hold 3rd Parties Accountable: Have contracts in place with vendors who transport and store your data
  - With indemnification and insurance.

Using Gmail & other Free E-mail Providers

- Use of Gmail to communicate or transmit personal information/confidential business information leaves the information open to vulnerabilities.
- Information sent via standard Gmail is not protected.
- Gmail terms state Google has access to all data transmitted through Gmail account.
- Google mines all data.
E-mail

- Encryption;
- Multi-factor authentication;
- Virtual Private Network (VPN)/RSA;
- Verify Selected Recipients;
- Use Standard Confidentiality Disclaimers in Outlook;
- "Sensitive" communications should be given special protections against disclosure to 3rd parties
- It is the responsibility of the employee directing the communication to determine if the communication is "sensitive" or "confidential."

Protect Paper Records

Protect high risk data:
- Any documents with SSN;
- W-2s;
- Health insurance records;
- Benefits records;
- Salary and personnel information;
- EFINs, PTINs, CAF.

How to protect high risk data:
- Lock filing cabinets;
- Lock offices/building/rooms;
- Only allow access by authorized personnel with a need to know;
- Do not send via regular mail;
- Implement a Data Retention Program;
- Destroy any paper records that don’t need to be kept/stored.

Know where your high risk data is, educate your employees, and follow your privacy and security plan to keep it protected!
Additional Resources

- IRS “Protect Your Clients; Protect Yourself”
  - www.irs.gov/tax-professionals/protect-your-clients-protect-yourself
- DHS CISA – Cybersecurity and Infrastructure Security Agency
  - www.cisa.gov/cybersecurity-division
- U.S. Secret Service
  - www.secretservice.gov/investigation/
- NIST – National Institute of Standards & Technology
  - www.nist.gov
- SANS Institute
  - www.sans.org

Thank you

QUESTIONS?
www.dataprivacyandsecurityinsider.com