IRS Nationwide Tax Forum 2020

Data Privacy and Cybersecurity for Tax Professionals

(advanced session)

SALVE REGINA UNIVERSITY
PELL CENTER *for* INTERNATIONAL RELATIONS *and* PUBLIC POLICY

Robinson+Cole

Agenda

1. Introduction
2. Security Challenges Related to COVID-19 Pandemic
3. Tips for Remote Working during COVID-19 Pandemic
4. Customer Data Makes You a Prime Cyber Target
5. Identify and Protect High Risk Data
6. Map Your High Risk Data
7. Understand What Laws Apply to Your Business
8. Enterprise-Wide Privacy and Security Compliance Program
9. Risks to Your Data – Phishing, Spear Phishing, Ransomware, Malware, Zero-Day Vulnerabilities
10. Develop an Incident Response Plan
11. Educate Your Employees
12. Basic Cyber Hygiene
13. Conclusion and Questions

Learning Objectives

At the end of this course, you will be able to:

- Identify and protect high-risk data.
- Recognize the signs of phishing, spear-phishing, ransomware, malware, and other cyber threats to the tax industry.
- Design a data privacy and security program fit for your business.
- Select appropriate security policies and processes to prevent, protect, mitigate, respond, and remediate cyber incidents.
- Develop an incident response plan and breach notification process.
- Understand the federal and state laws that apply to your business.
- Adopt cyber hygiene best practices.

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 a data breach is critical to protect your clients and your business.

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.

Cybersecurity matters to countries, organizations, and individuals now more than ever during this crisis!

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- Unpatched and out-of-date systems, and IoT (Internet of Things) devices at home enabled and listening (e.g., home security cameras, Alexa, etc.)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 COVID19-themed phishing messages to conduct ransomware attacks or implant malware;
- Large-scale stimulus fraud and stimulus-themed spear-phishing campaigns;
- Increased collection of health information from employees (e.g., temperature checks, answers to screening questions, contact tracing apps).

Tips for Companies with 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, if you are subject to HIPAA, 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.

Tips for Companies with Remote Workers (cont'd)

- **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 provide security reminders for phishing, etc.
  - Refresh employees on privacy and security measures and incident reporting requirements.
  - Also, conduct a remote mock incident response.
  - SANS remote work toolkit.

Tips for Companies with Remote Workers (cont'd)

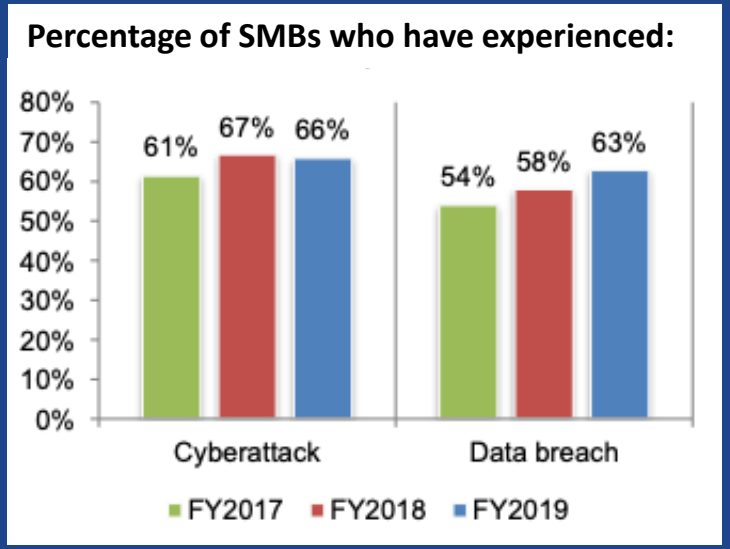
- **No Document Printing**
  - A home environment is not the best for paperwork. Restrict printing unless absolutely necessary. Where it is necessary, require shredders or offer a shred-at-work solution using a dedicated shred box at home.
- **Document Sharing and Storing**
  - In order to assist with no document printing, develop or enforce a document sharing protocol. Restrict or permit as necessary cloud storage tools. People will tend to retain everything, and it may not be needed. Encourage minimum document retention and advise employees to check temporary storage and downloads.

Tips for Companies with Remote Workers (cont'd)

- **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.

Customer Data Makes You a Prime Cyber Target!

- The percentage SMBs that experienced a data breach grew from 58% in 2018 to 63% in 2019.
- More than 60% of SMBs said the cause of the incident was a negligent employee or contractor.
- Attacks are becoming more sophisticated, with phishing (57%), compromised or stolen devices (33%), and credential theft (30%) among the most common attacks waged against SMBs globally.
- The average cost of cyber attacks on SMBs reached $3.1 million in 2019, with an average cost due to damage or theft of IT assets or infrastructure of over $1.2M, and an average cost for disruption to normal business operations of more than $1.9M.
- An estimated 60% of SMBs will go out of business within 6 months of a cyber attack.



2019 Global State of Cybersecurity in Small & Medium Sized Business
Ponemon Institute, 2019

The number one cause of cyber breaches are a company's own employees!

Finding a Balance Between Privacy and Convenience

- 200 billion IoT devices expected by 2025.
- Interaction with an online device every 18 seconds vs. 6.5 minutes today.
- We will generate 10x more data, sharing and exposing more while protecting less.
- We will continue to choose convenience over privacy/security.
- "Free" is not free when you provide personal information.
- As technology advances, so will the prevalence and scope of cyberattacks.

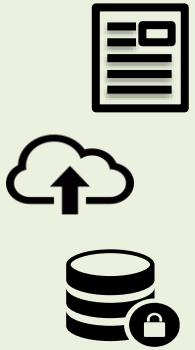
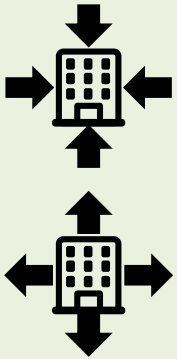
STEP 1: Identify and Protect High-Risk Data

Personally Identifiable Information	Name & Contact Information	Personal Characteristics & Health & Ins Acct Information	Financial Data & Employment Information
Social Security # State-issued ID # Driver's license # Passport # Mother's Maiden Name Credit history Criminal history	Initials Address Telephone number E-mail address Mobile number Date of birth EFINs / PTINs / CAF #	Age Gender Marital status Nationality Insurance account # Prescriptions Medicare and Medicaid information	Credit, ATM, debit card #s Bank Accounts Security/Access Codes Passwords Income/Salary Service fees Compensation info Background check info

To assist tax professionals in protecting sensitive data, the IRS created multiple videos and other resources:
www.irs.gov/newsroom/security-summit-urges-tax-pros-to-protect-their-identification-numbers-efins-ptins-and-caf-numbers

STEP 2: Map Your High-Risk Data

- Determine where your high risk data is stored, where it is going, who has access to it, and the overall **data flow** so that you know how to protect it (and who to protect it from).

What Media?	Where is it located?	What's the value?	Is it encrypted?	Where does it go?
		$ $$ $$$ $$$$ $$$$$	Yes No	?

STEP 3:
Understand the Laws that Apply to Your Business

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

What Can you Do to Follow applicable Laws, Regulations and Guidelines?

MINIMIZE the risks of an attack

MONITOR for dangers

MANAGE the damage

MINIMIZE: Enterprise-Wide Privacy + Security Program

- Set clear policies, procedures, and standards;
- Foster education through training and awareness, not just on phishing but also around new cyber risks – or old ones that are more prominent now – (e.g., is Alexa recording your sensitive conference calls?);
- Ensure compliance with regulatory and legal requirements;
- Audit and assess periodically;
- Assess collection, use, and disclosure of data;
- Examine the processing and storage of data;
- Implement appropriate security processes to protect the transmission of data;
- Establish website privacy policy and terms of use, privacy policy, and security policy and procedures.

MINIMIZE: Employees Need to Know - 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.

MONITOR: Consider the Risks to Your Data

- **Phishing:** A malicious "spam-like" message sent in large batches to a broad audience.
- **Spear-Phishing:** A form of phishing – messages appear to come from a familiar or trusted sender and target recipients.
- **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Malware:** Software that is intended to damage or disable computers and computer systems.
- **Zero-Day Vulnerability:** A yet unknown or newly discovered software vulnerability. Because the developer is either unaware or 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.

Ransomware

Ransomware is a type of malware that restricts access to an infected computer system

- Demands ransom to unlock system and remove restrictions;
- Some forms systematically encrypt files on the system's hard drive;
- Difficult or impossible to remove 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;
- Paying the ransom doesn't always work – you're dealing with criminals.

How to avoid ransomware infections:

- Don't click on unknown links or open suspicious attachments that you weren't expecting to receive or that seem odd;
- Keep your anti-virus software up to date;
- Back up all important information;
- Educate all employees (cyber hygiene).

MAZE Ransomware

- In January 2020, FBI warned U.S. companies of Maze ransomware attacks, in which attackers impersonate government agencies, well-known security vendors, and other seemingly trustworthy organizations to infiltrate victim networks;
- French government cybersecurity agency recently published a Maze alert;
- Maze uses multiple methods for intrusion;
- Maze actors steal and encrypt data and then threaten to publicly release confidential and sensitive files in an effort to ensure ransom payment;
- Law firms, medical providers, City of Pensacola, and other municipalities and businesses targeted in recent Maze attacks.

REvil Ransomware

- This latest ransomware gang (Sodinokibi) pressures victim companies to pay ransom by publishing files and threatening to release more data until the ransom demand is met. (reported by Krebs On Security)

- The criminal group is threatening to release files from a NY law firm regarding the firm's celebrity clients unless they pay a $42 M ransom demand. (reported by ZDNet)

- The gang recently launched an eBay-like auction site where they plan to sell data stolen from the companies they hack. (reported by ZDNet)

What is a Zero-Day Vulnerability?

- A software vulnerability in a system or device that has been discovered but is not yet patched – the developer/vendor is either unaware or hasn't released a fix for the vulnerability yet.
- An exploit that attacks a zero-day vulnerability, before a vendor can issue a "patch," is called a zero-day exploit.
- Cybercriminals race to exploit these vulnerabilities to cash in on their schemes.
- Vulnerable systems are exposed until a patch is issued by the vendor.
- Cynet reports that half of the malware attacks detected in 2019 were zero-day threats.

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.

NIST Security Bulletin Re: Telework

A recent NIST Security Bulletin provides guidelines on telework and remote access to help mitigate security risks

"Security for Enterprise, Telework, Remote Access, and Bring Your Own Device (BYOD) Solution"
https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

IoT Devices – Is Alexa 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.

BYOD Programs

- 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

- Ensure 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.

Collecting Health Data from Employees

- Usually involves health data not covered by the Health Insurance Portability and Accountability Act (HIPAA)
  - Temperature checks or answers to screening questions;
  - Use of a contact tracing apps.
- Other federal laws may determine what a company can do with employee health data such as the Americans with Disabilities Act (ADA) or the Family Medical Leave Act (FMLA)
  - Data collection and use should be transparent, and data should be collected, stored, and protected only for as long as necessary.
- Strike a balance between employee privacy and employee safety.

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.

MANAGE: 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.)

MANAGE: Educate Your Employees

- Make employees aware of the important role they play in privacy and security.
- Your employees are your front line of defense when it comes to security (but also one of your highest risks).
- Companies should create a culture of privacy and security from the board room to the mail room, and make cybersecurity training an on-going process.

How do you better protect your data beyond the enterprise-wide data privacy & security program?

MINIMIZE

MONITOR

MANAGE

IRS Nationwide Tax Forum | 2020

Cyber Hygiene Best Practices

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.

IRS Nationwide Tax Forum | 2020

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

IRS Nationwide Tax Forum | 2020

AMERICAN COALITION FOR TAXPAYER RIGHTS

This seminar was made possible thanks to a generous grant from the American Coalition for Taxpayer Rights (ACTR) to the Pell Center at Salve Regina University

SALVE REGINA UNIVERSITY

PELL CENTER *for* INTERNATIONAL RELATIONS *and* PUBLIC POLICY

Thank You / Questions

Linn Foster Freedman
Partner
Robinson + Cole
Email: lfreedman@rc.com
Blog:
www.dataprivacyandsecurityinsider.com

Our Mission
We cultivate deep relationships within our communities, the legal profession and industries we serve to envision "the whole picture" and to understand the factors that drive today's constantly changing world.

Francesca Spidalieri
Sr. Fellow for Cyber Leadership
Pell Center, Salve Regina University
Email: pellcenter@salve.edu

Our Mission
We are a multidisciplinary research center focused at the intersection of politics, policies and ideas.

Robinson+Cole

SALVE REGINA UNIVERSITY
PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY