IRS Nationwide Tax Forum 2023

Cybersecurity for Tax Professionals

(Advanced Session)

Rev. 6/29/2023

Learning Objectives

- Understand cybersecurity threats and common cyber risks to the tax industry
- Recognize the signs of fraud, scams, ransomware, phishing, smishing, QRishing, third-party compromise, and other common cybersecurity risks to the tax industry
- Identify, map, and protect high-risk data, including clients and employees' PII
- Design a data privacy and security program fit for your organization
- Select appropriate security measures to prevent, protect, mitigate, respond to, and remediate cyber incidents and intrusions
- Develop a cyber incident response plan and data breach notification process
- Understand the federal and state laws that apply to your business
- Adopt cyber hygiene good practices
- Understand your responsibilities for the overall cybersecurity and cyber resilience of your organization, including policy development, implementation, and communication

IRS Nationwide Tax Forum 2023

Introduction

Every tax professional — whether a member of a major accounting firm or an owner of a one-person storefront — is a prime target for highly sophisticated, well-funded, and technologically adept cybercriminals around the world. Why? Your clients' information (e.g., bank and investment accounts, SSNs, health insurance records, etc.) can be a virtual goldmine in the wrong hands, allowing criminals to file fraudulent tax returns that better impersonate their victims and are harder to detect. That's why securing it against a data breach is critical to protect your clients and your business.

Protecting client data also is the law!

Evolving attack landscape

- **In the past…**

  …bad actors specialized predominantly within their own areas of expertise and were loosely organized groups targeting individuals.

- **In today's environment…**

  …criminals are highly skilled, well-resourced networks of threat actors targeting technology assets of large corporations as well as small businesses ("low-hanging fruits") and their interconnected infrastructure, vendors, and clients.

IRS Nationwide Tax Forum 2023

Current Trends in Cybersecurity Threats

In 2022, it took an average of 277 days – about 9 months – to identify and contain a breach (and 49 days longer to identify and contain ransomware attacks, which grew by 41%).

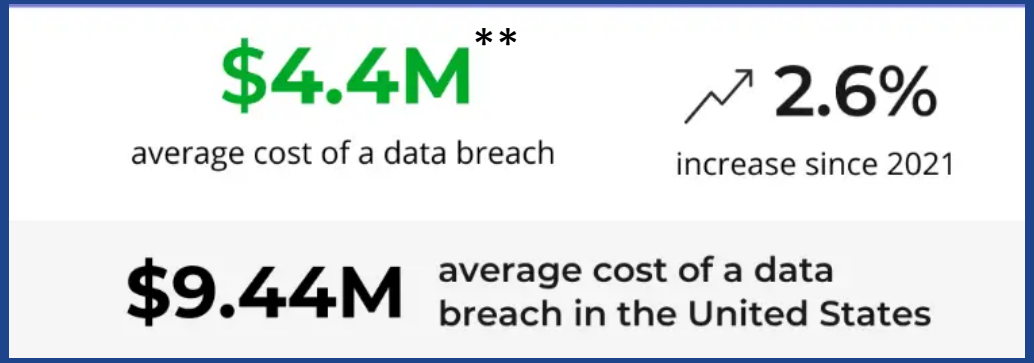
The top 3 most common attack vectors are:

1. Stolen or compromised credentials (19%)
2. Phishing (16%)
3. Cloud misconfigurations (15%)

(*2022 Cost of a Data Breach report*)

IRS Nationwide Tax Forum 2023

Average Cost of a Data Breach in 2022



The average cost was $1 million higher in breaches where remote working was a factor in causing the breach, compared to those where remote working was not a factor.

***highest average ever recorded*

(*2022 Cost of a Data Breach report*)

Growing Cybersecurity Threats

The fact that technology is constantly advancing isn't a new phenomenon, but the cyber threat landscape has been growing exponentially in the last few years.

The word "disruption" adequately described the experiences of countless organizations during the COVID-19 pandemic — no one could have predicted its impact on business, technology, and cyber risk management.

Emerging Cybersecurity Threats

- Unintended disclosures by employees (employee error)
- Hacking
- Malware
- **Ransomware**
- Insider Wrong-Doing
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/Removable Media

Emerging Cybersecurity Threats (cont'd)

- Technology Intrusions
- Phishing/Spear-Phishing/Smishing
- Vishing/QR-ishing Schemes
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors – Poor Security Protocols/Standards

IRS Nationwide Tax Forum 2023

IRS

What data does your organization need to protect?

What are malicious threat actors after?

High-Risk Data in a Highly Connected World

- Social Security numbers;
- Driver's license numbers or state-issue identification card numbers;
- Passport numbers;
- EFINs/CAF numbers;
- e-Services passwords;
- Alien registration or tribal identification number;
- Financial account numbers, credit card numbers, or debit card numbers 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.

IRS Nationwide Tax Forum 2023

High-Risk Data in a Highly Connected World

- 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.

IRS Nationwide Tax Forum 2023

IRS

What is the biggest risk right now?

Ransomware

- Ransomware is a type of malicious software that encrypts systems and files and restricts access to infected computer systems. Malicious actors use multiple methods for intrusion, including phishing and other malware. They then threaten to publicly release the victim's data and/or perpetually block access to it unless a ransom is paid (usually in Bitcoin or other cryptocurrencies).
- 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 compromised employees/customers.

IRS Nationwide Tax Forum 2023

What Happens During a Ransomware Attack?

- Malicious actors demand 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 malicious links or attachments to an email message (phishing) 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.

IRS Nationwide Tax Forum 2023

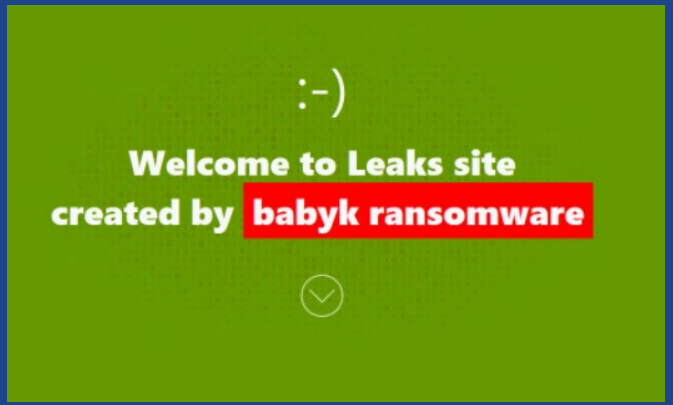
Recent Ransomware Statistics

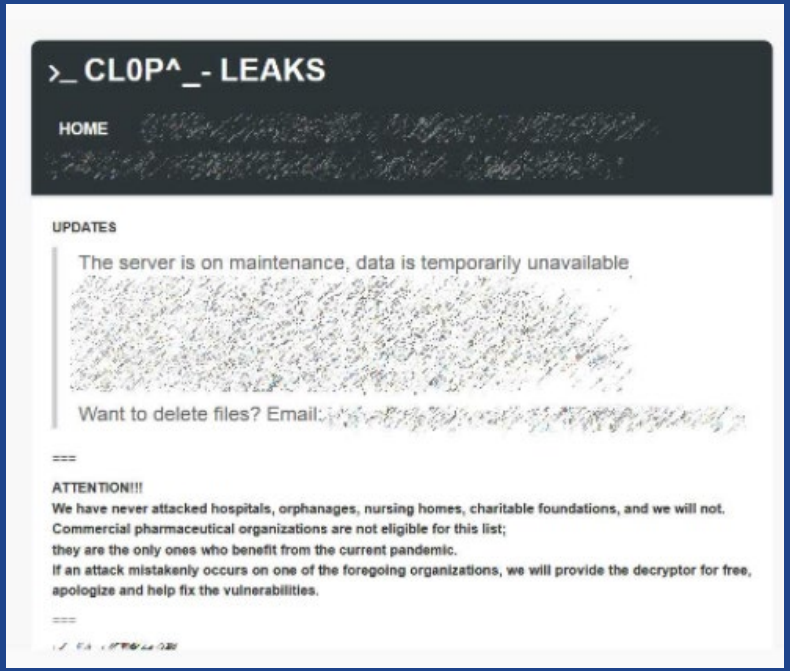
- In 2022, the average cost of a ransomware attack (not including the cost of the ransom itself) was $4.54M*, with an *initial demand* of over $1 million in ransom (an all time high).**
- According to Coveware, in the 1st quarter of 2023, the top 5 ransomware variants were: BlackCat, Black Basta, Royal, Hive, Lockbit 3.0, Phobos, and BinLian.**
- 77% of ransomware attacks leveraged data exfiltration ('double extortion tactic') – a more efficient, less disruptive way to extort companies without attracting law enforcement attention.**

*2022 Ponemon Report
**Coveware, 1st Quarter 2023 Report

Public Shaming Websites

- Many ransomware operators have created data leak sites to publicly shame their victims and publish the files they stole.





What are the Effects of these Threats?

- Traditional cyber threats to businesses present a range of damages that include reputational damage, financial losses and fraud, lost productivity, recovery costs, and serious damage to businesses that could be catastrophic.
- Potential to remotely access and damage physical systems is another threat.
- Cripple government services/functioning (i.e., Costa Rica)

The above-noted threats, if they occurred in businesses critical to the financial services sector, could shut down or slow supply chains, hurt the financial sector, and wreak havoc on businesses of all sizes.

IRS Nationwide Tax Forum 2023

How to Avoid Phishing and Ransomware attacks

- Be aware of any urgent message or confidential requests.
- Think before replying – Never “reply” or click on unknown links in emails containing a suspicious request or open suspicious attachments in emails that you weren’t expecting to receive or that seem odd.
- Authenticate the sender of the message by contacting them by an alternative method (phone) before sending sensitive information or authorizing transactions.
- Update and patch systems and make sure security solutions are up to date.
- Educate all employees about the potential impact of online scams (cyber hygiene).
- Consider whether or not to pay online extortion demands — payment encourages crime and you might not get your data back anyway!
- Be mindful of what you share on social media and update your privacy settings.
- Install and enable remote wiping and/or remote disabling of computer devices.
- Alert your bank of potentially fraudulent transactions or suspicious activity on your credit card.

Robust Backup Systems: Why they are important

- As important as security safeguards might be, backups are ultimately the only thing that can save an organization's data after a ransomware attack has already occurred.
- Having an offline backup copy acts as a stopgap. Ransomware cannot touch a backup IF it is disconnected from the system.
- Keeping a backup copy of vital data is a good way of reducing the damage of a ransomware attack – it allows companies to get systems up and running again without having to pay off the cyber criminals.
- In addition, it might not be enough just to back up the important data and documents. Entire machines may need to be backed up, if they are critical to the business.

IRS Nationwide Tax Forum 2023

CISA Recommendations to Reduce the Risk of Ransomware

In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) launched the Reduce the Risk of Ransomware campaign with information and resources for individuals and organizations to implement "smart cyber habits" to avoid falling victim of ransomware, including:

1. **Keep Calm and Patch On** – Patching is essential for preventive maintenance that keeps machines up-to-date, stable, safe, and secure against malware and other cyber threats.
2. **Backing Up Is Your Best Bet** – It is critical to set up offline, encrypted backups of data and to regularly test your backups. The more you automate your backup system, the more frequently you can back up your data.
3. **Suspect Deceit? Hit Delete.** – If an email looks suspicious, do not compromise your personal or professional information by responding or opening attachments. Delete junk email messages without opening them.
4. **Always Authenticate** – Implement multifactor authentication (MFA) to prevent data breaches and cyber-attacks. This includes a strong password and at least one other method of authentication.

CISA Recommendations (cont'd)

5. **Prepare and Practice Your Plan** – Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
6. **Your Data Will Be Fine If It's Stored Offline** – Local backups, stored on hard drives or media, provide a sense of security in case any issues occur. Keep your backup media in a safe and physically remote environment.
7. **Secure Your Server Message Block (SMB)** – SMB vulnerabilities allow their payloads to spread laterally through connected systems like a worm. IT professionals should disable their SMB protocols to prevent malware attacks.
8. **Paying Ransoms Doesn't Pay Off** – The U.S. government recommends against paying ransom to cybercrime organizations or malicious cyber actors. Paying a ransom only funds cybercriminals and there is no guarantee you will recover your data if you do pay.
9. **Ransomware Rebuild and Recovery Recommendations** – Identify the systems and accounts involved in the initial data breach and conduct an examination of existing detection or prevention systems. Once the environment is fully cleaned and rebuilt, issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility.

IRS Nationwide Tax Forum 2023

IRS Recommendations to Minimize Cyber Risks and Prevent Identity Theft

- Develop data security plans to prevent, protect from, and counter identity theft:
  - Identify & protect your high-risk data (e.g., SSNs, IDs, DoB, e-mails & passwords, EFINs/CAF #, Credit/ATM/debit cards, bank accounts, insurance accounts).
  - Determine where your high-risk data is stored (e.g., on-premise servers, USB flash drive, hard disk drive, cloud-base storage, paper records), where it is going, who has access to it, and the overall data flow so that you know how to protect it (and from whom).
- Develop a cybersecurity strategy to better combat fraud and protect clients' data.
- Know the signs of identity theft; take action if you're a victim:
  - See "IRS Taxpayer Guide to Identity Theft"
- Develop incident response plans to mitigate, respond, and remediate cyber incidents, identity theft, and other data breaches.

To assist tax professionals in protecting sensitive data, the IRS has 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

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**
- **Policies and procedures as legally required to address**
  - Privacy
  - Security
- **Technology to secure it**
  - Encryption
  - Firewalls
- **Educate users and employees**

Vendor Management

- **Map all vendors who have access to personal information**
  - Follow the data

- **Put agreements in place with robust privacy and security requirements with each vendor:**
  - Payroll/HR
  - Benefits/insurance
  - Website hosting provider
  - Cloud service provider
  - IT service providers
  - Legal

Privacy & Security Policies, Procedures, and Standards

- Most states require businesses to have safeguards for protecting personal information and when to dispose of such data.
- The IRS recommends having a data security plan in place (IRS tax tip 2019-174)
  - Tax Security 2.0- A "Taxes-Security-Together Checklist – IRS urges tax professionals to review practices, enhance safeguards to protect taxpayer data.

Develop an Incident Response Plan

1. 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

2. 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)

Develop an Incident Response Plan (cont'd)

3. Determine who are the stakeholders:
   - Organizational leadership
   - IT & Information Security leadership
   - Audit
   - Finance
   - Human Resources
   - Communications
   - Legal counsel

4. Compile the following information NOW:

   Obtain and select insurance approved vendors (as appropriate) and maintain updated contact information for:
   - Forensic vendors
   - Credit monitoring/call center/identity theft mitigation services vendors
   - Outside legal counsel
   - Cyber insurance company to report breach/security incident
   - Law enforcement officials, including state and federal officials
   - Applicable regulatory body
   - Information sharing entities

5. Determine what decisions need to be made:
   - Obtain or clarify cyber liability insurance information and requirements
   - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services

6. Distribute the Plan and Review it at least once a Year + Conduct Tabletop Exercises

IRS Nationwide Tax Forum 2023

Understand the Laws that Apply to Your Business

- IRC Regulations
- State Data Breach Notification Law(s)
- State Laws Applicable to Tax Preparers
- Data security laws and data protection laws
- Available guidelines, frameworks, and benchmarks.

Changing Legal Landscape

- California Consumer Privacy Act (CCPA)
  - California Privacy Rights Act (CPRA) amendments
  - Some exceptions/exemptions (e.g., GLBA)
  - Employee notice required (limited rights apply to employees)
- Virginia Consumer Data Protection Act
- Colorado Privacy Act
- Utah Consumer Privacy Act
- Connecticut Data Privacy Act
- Tennessee, Montana, Iowa, + Indiana have passed consumer privacy statutes
- Many other states have privacy laws pending

IRS Nationwide Tax Forum 2023

IRS

Practicing Cyber Hygiene

Mobile Devices and Apps

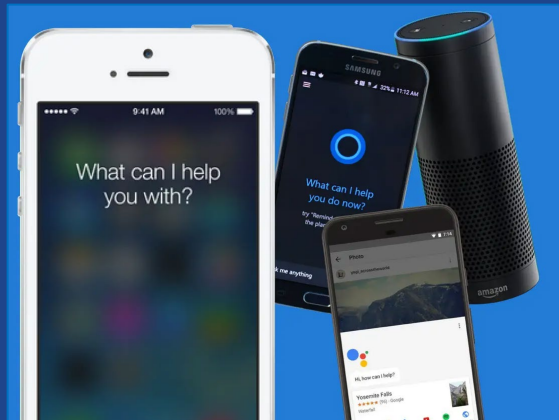
- PRIVACY SETTINGS
  - Location, microphone

Vishing, Smishing & QRishing

- Exploits via SMS, telephone calls, or text messages
- Vishing:
  - Often the caller will pretend to be calling from the government, tax department, police, or a bank, requesting personal information.
- Smishing:
  - Text messages with malicious links to webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number.
- QRishing:
  - Form of phishing initiated using malicious QR codes embedded in emails, texts, posters, magazines, brochures, or menu-less restaurants.
- Cyber criminals want this integration of email, voice, text message, & web/mobile browser functionality to increase the likelihood that users will fall victim to social engineering and other malicious activities.

Telework-related Cyber Risks & IoT Devices

- Distracted employees
- Clicking on potentially malicious links and attachments
- Using unsecure Wi-Fi connections
  - Must use a secure Wi-fi and VPN connection
  - Use strong passwords for home 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
- Is the data properly and regularly backed up?
- IoT devices (Alexa, Siri, Cortana) 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.

  - 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 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.
- **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.
  - Regularly review IR Plan & conduct remote mock incident response/tabletop exercises.

Cybersecurity Practices to Protect Data at Rest and in Transit

- Implement a process for addressing and fixing cybersecurity issues (e.g., identify possible gaps in security in the information sharing process).
- Determine whether the appropriate level of cyber liability insurance is in place (both the employer and vendors) to help mitigate the damage of any potential attack and be sure that such coverage is as broad as possible.
- Document the process for moving plan data, maintain a data inventory, retain only data needed and, if data elements can be redacted, do so.
- Delete records that are no longer necessary and make sure providers do the same.
- Consider retaining an outside firm that specializes in cybersecurity to confirm that data is secure through periodic audits.
- Implement processes and controls to restrict access to systems, applications, data and other sensitive information.
- Utilize multi-factor authentication to access client accounts and data.

Cybersecurity Practices to Protect Data at Rest and in Transit (cont'd)

- Develop a cybersecurity risk management strategy to address your response to a potential breach (including appropriate notices and remediation efforts).
- 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:
  - Malicious actors have devised viruses and worms that specifically target USBs;
  - So small they're easy to lose/get stolen;
  - If a lost or stolen USB drive contains sensitive personal information that's not encrypted or secured, it could be a reportable data breach.

IRS Nationwide Tax Forum 2023

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

- Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.
  - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity.
- Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented.
  - Look for contract provisions that give you the right to review audit results demonstrating compliance with standard.
- When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware of contract provisions that limit the service provider's responsibility for IT security breaches:
  - Information Security Reporting
  - Clear Provisions on the Use and Sharing of Information and Confidentiality
  - Notification of Cybersecurity Breaches
  - Compliance with Records Retention and Destruction, Privacy and Information Security Laws
  - Insurance

Secure Connected Devices and Email Communication

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.

Connected Devices and Email Communication (cont'd)

- Enable encryption
- Use multi-factor authentication to log into emails, VPNs, databases
- Virtual Private Network (VPN)/RSA
- Verify Selected Recipients
- Check your sent mail, junk mail, and email account settings regularly – hackers often compromise email accounts first and modify the "email forwarding" settings to forward emails to their own account
- Use Standard Confidentiality Disclaimers
- Avoid email as a method for sending sensitive or confidential information – use a secure (encrypted) document sharing or transaction management platform
- "Sensitive" communications should be given special protections against disclosure to third-parties
    - It is the responsibility of the employee directing the communication to determine if the communication is "sensitive" or "confidential."

IRS Nationwide Tax Forum 2023

Privacy Issues and Employee Training

- Understand and improve workplace dynamics and value cultural competence – which can help to mitigate risks of insider threats.*
- 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.

*Center for Development of Security Excellence's Understanding the Intersection of Cultural Competence and Organizational Risk.

Additional Resources

- **IRS "Safeguarding Taxpayer Data"**
  - https://www.irs.gov/individuals/data-theft-information-for-tax-professionals
- **IRS "Protect Yourself, Protect Your Clients" Campaign**
  - https://www.irs.gov/tax-professionals/protect-your-clients-protect-yourself
- **Cybersecurity and Infrastructure Security Agency (CISA)**
  - https://www.cisa.gov/cybersecurity-division & https://www.cisa.gov/stopransomware/reduce-risk-ransomware-campaign-cisa
- **U.S. Secret Service Cyber Crime Investigations**
  - https://www.secretservice.gov/investigation/cyber
- **NIST Cybersecurity Framework (CSF)**
  - https://www.nist.gov/cyberframework
- **SANS Institute**
  - www.sans.org

IRS Nationwide Tax Forum 2023

IRS

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

IRS Nationwide Tax Forum 2023

Contact Information

Linn Foster Freedman
Partner
Chair Data Privacy + Security Team
Robinson + Cole
Email: lfreedman@rc.com
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.

Kathryn Rattigan
Partner
Data Privacy and Security Team
Robinson + Cole
Email: krattigan@rc.com
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
Website: www.pellcenter.edu
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