



2024



IRS Nationwide
TaxForum

Cybersecurity for Tax Professionals

Advanced Session



Learning Objectives

Understand cybersecurity threats and common cyber risks to the tax industry

1

Recognize the signs of common cybersecurity risks to the tax industry

2

Identify, map, and protect high-risk data, including clients and employees' PII

3

Design a data privacy and security program fit for your organization

4

Select appropriate security measures to prevent, protect, mitigate, respond to, cyber incidents and intrusions

5

Develop a cyber incident response plan and data breach notification process

6

Understand the federal and state laws that apply to your business

7

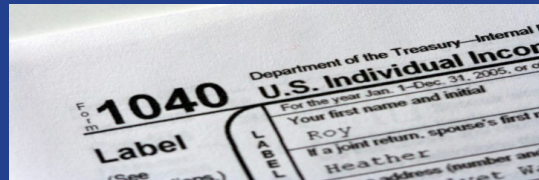
Adopt cyber hygiene good practices

8

Understand your responsibilities for the overall cybersecurity and cyber resilience of your organization

Introduction

- You are a prime target for **sophisticated** and **well-funded** cybercriminals.
- Why? Your clients' information (e.g., bank and investment accounts, SSNs, health insurance records, etc.) is **VALUABLE** to them.
- Tax professionals have an ethical and legal obligation to protect client data.



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 and 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.



Common Threats to Tax Professionals

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



Common Threats to Tax Professionals

- Social Engineering
 - Phishing/Spear-Phishing
 - Smishing/Vishing
 - QRishing
- MFA Fatigue Attacks
- Wire Transfer Fraud (often resulting from Business Email Compromise)
- Vendors/Subcontractors – Poor Security Protocols and Standards



Average Cost of a Data Breach in 2023

- \$4.45 million Globally
- \$9.48 million Domestically
- 6 Costliest Attack Vectors:
 1. Malicious Insider: \$4.9 million
 2. Phishing Attacks: \$4.76 million
 3. Business Email Compromise: \$4.67 million
 4. Stolen/Compromised Credentials: \$4.62 million
 5. Other Social Engineering: \$4.55 million
 6. Lost/Stolen Device: \$4.46 million (2023 IBM Ponemon Report)





Higher Cost Attacks Take Longer to Contain

Time to identify and contain a data breach by initial attack vector

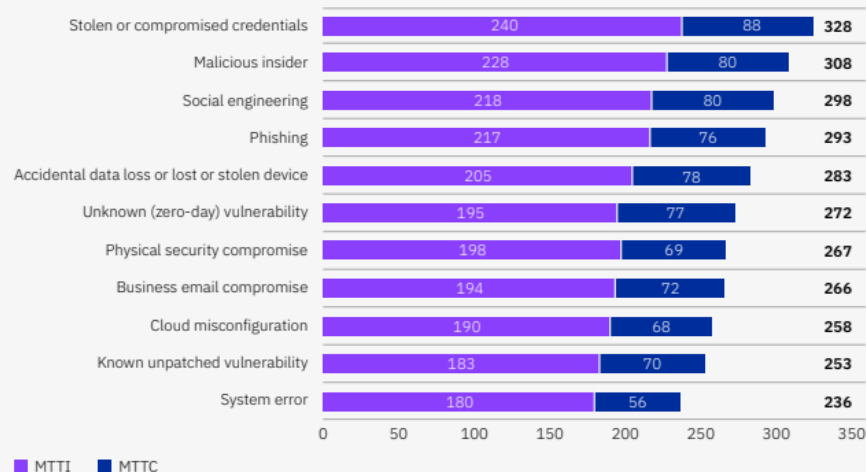


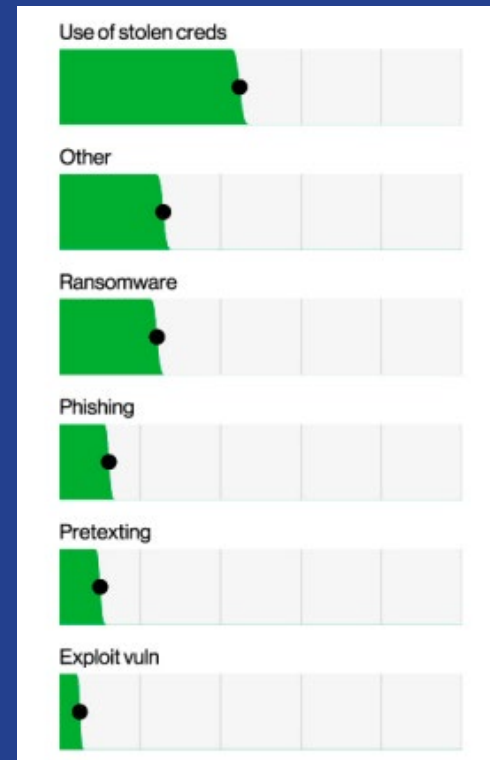
Figure 11. Measured in days



Top Attack Methods (2023 Verizon Report)

Stolen Credentials, Ransomware, and Phishing topped the list of common attack methods.

Social engineering (i.e. – phishing, pretexting) continues to have more impact than exploiting technological vulnerabilities.





Phishing, Vishing, and Smishing

These are targeted social engineering exploits achieved via Email SMS, telephone calls or text messages.

Cyber criminals want this integration of email, voice, text message, and web browser functionality to increase the likelihood that we will fall victim to engineered malicious activity.

When in doubt, verify any suspicious messages through trusted channels.

Do not engage with suspicious messages.



Phishing, Vishing, and Smishing

- **Phishing**
 - Emails may purport to be from trusted sources, such as a company executive or IT and HR personnel
 - Pay close attention for ever-so-slightly off source addresses and “[External]” tags on messages
 - Whaling is a subset of phishing targeting C-level executives
- **Vishing**
 - Often the caller will pretend to be calling from the government, tax department, police, or a bank, requesting personal information
- **Smishing**
 - Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number





QRishing

- Using QR Codes in emails and texts
- Embedded malicious code within QR Code
- Comfortable with QR Codes from menu-less restaurants during pandemic
- Same results as phishing, vishing and smishing



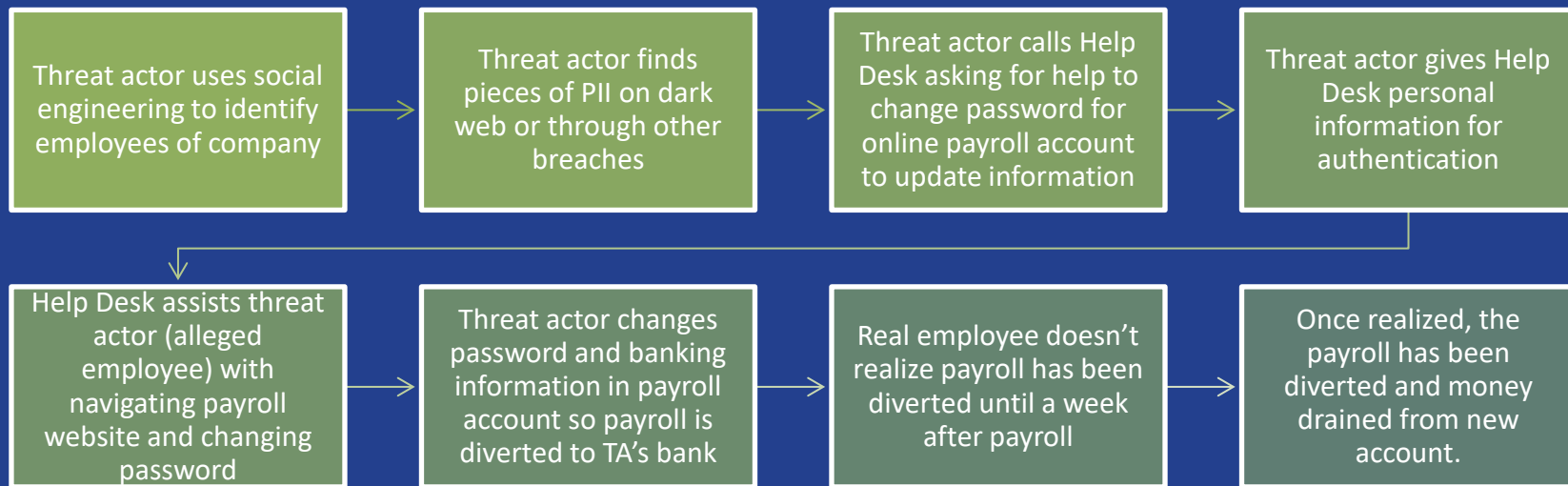


Smishing in the News: NYC Payroll Administration

- The Mayor's administration took the NYCAPS payroll website offline due to a phishing attack targeting city employees' personal information.
- Employees received scam text messages asking them to activate multi-factor authentication for the NYCAPS system.
 - Directed employees to a fake website prompting them to enter usernames, passwords and even a picture of their driver's license.
- Roughly 300,000 city workers lost access to essential tax forms.



Real Vishing Attack Against Helpdesks



How to Avoid Phishing

- Be aware of any urgent message or confidential requests.
 - Do not engage with suspicious message.
 - Authenticate the sender of the message by contacting them by an alternative method (phone) before sending sensitive information or authorizing transactions.
 - Report suspicious messages to IT.
- Educate all employees about the potential impact of online scams. (cyber hygiene)
- Be mindful of what you share on social media and update your privacy settings.



Data Mapping and Risk Assessment

- 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
- Bank account numbers, credit card numbers, etc.





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





What is still the biggest risk?





Ransomware



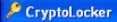
- Ransomware is malicious software that encrypts systems and files without your consent.
- Criminals use multiple methods for intrusion, including phishing and malware.
- They then threaten to publicly release the victim's data and/or block access unless a ransom is paid (usually cryptocurrency).
- Broad categories of resulting costs
 - Lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for compromised employees/customers.



What Happens During a Ransomware Attack?

- Criminals demand ransom to remove the restrictions
 - It is difficult or impossible to decrypt without paying the ransom
 - Some pseudo-ransomware may simply lock the system and display messages to coax the user into paying
- Most ransomware enters the system via malicious links or attachments to an email message (phishing) or through a zero-day vulnerability





Your personal files are encrypted!



Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>



Payment for private key



Private key will be destroyed on
9/20/2013
6:48 PM

Time left
71 : 57 : 22

Choose a convenient payment method:
Bitcoin (most cheap option)


bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

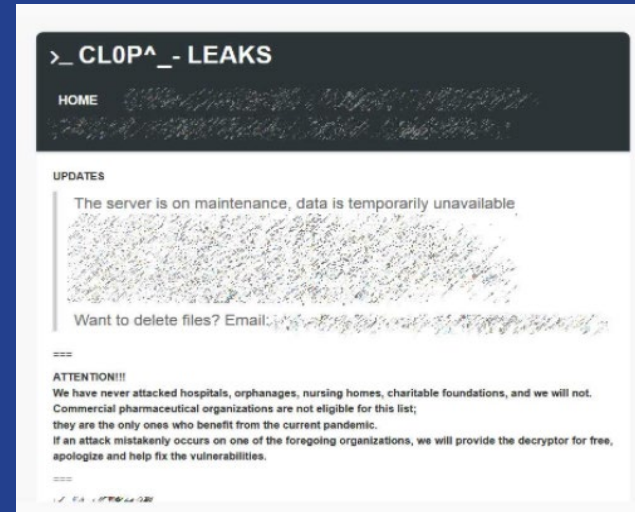
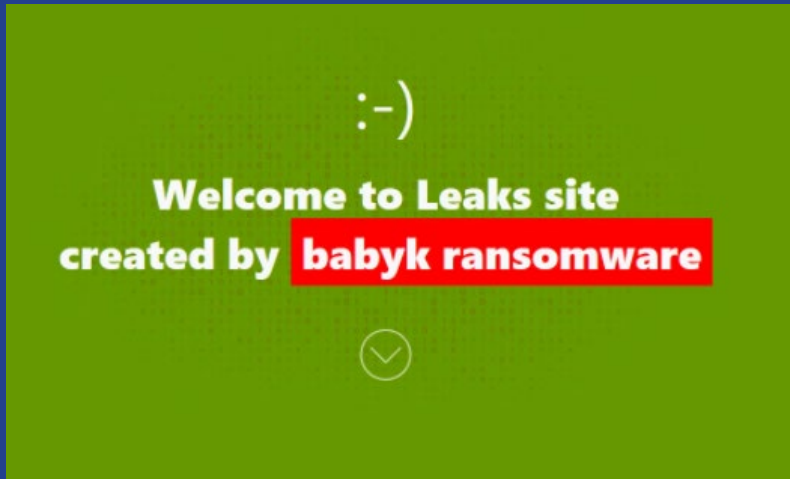
2 BTC

<< Back

PAY

Public Shaming Websites

- Cybercriminals will “name and shame” companies online to create pressure to pay the ransom
- They may also reach out directly to individuals affected by the breach



Robust Backup Systems

- Backups are the only way to restore your data without paying the ransom.
- Backups should be kept offline/air-gapped
- Consider business continuity: what files, documents, and systems are critical for business function?



CISA Recommendations to Reduce the Risk of Ransomware



PROMPTLY APPLY
SOFTWARE PATCHES.



APPLY AUTOMATED
BACKUPS.



DO NOT ENGAGE WITH
SUSPICIOUS EMAILS AND
REPORT THEM TO IT.



IMPLEMENT
MULTIFACTOR
AUTHENTICATION (MFA)



CISA Recommendations to Reduce the Risk of Ransomware



CREATE, MAINTAIN, AND
EXERCISE AN INCIDENT
RESPONSE PLAN



MAINTAIN SECURE
OFFLINE BACKUPS



DISABLE SMB
PORTS TO REDUCE
MOBILITY OF
WORMS



CONDUCT
REGULAR
SECURITY AUDITS



ENFORCE STRONG
PASSWORDS



*CISA ADVISES AGAINST
PAYING RANSOM*





IRS Recommendations to Minimize Cyber Risks and Prevent Identity Theft

- Determine where high-risk data is stored, where it is going, who has access to it, and the overall data flow
- Develop a cybersecurity strategy to better combat fraud and protect clients' data.
- Know the signs of identity theft & act if you're a victim:
- Develop incident response plans to mitigate, respond, and remediate cyber incidents, identity theft, and other data breaches.

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



Be Prepared for a Breach

- Create a comprehensive information security plan:
 - Risk assessment (organization's most critical assets & data flow)
 - Written Information Security Program (WISP)
 - Incident Response Plan
 - Trigger events (how to identify/verify intrusion)
 - Mitigation plan (minimizing damages)
- Identify State & Federal Laws and Requirements
 - 50 State Breach Notification Laws





Develop an Incident Response Plan



Identify Stakeholders

- Organizational leadership
- IT & Information Security leadership
- Audit
- Finance
- Human Resources
- Communications
- Legal counsel



Retain Insurance-Approved Vendors

- 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

Enterprise-Wide Privacy & Security Program

- Conduct a security risk assessment
- Implement legally required policies and procedures to address privacy & security
- Educate employees and other users – Training and Phishing Testing



Protect Enterprise Data

Paper data

- Store in locked areas
- Retain only as necessary
- Segregate highly sensitive data

Electronic Data

- Access controls & user authentication
- Encryption
- Firewalls



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)
- Many states recently passed similar laws:
 - VA, CO, CT, UT, OR, TX, FL, MT, IA, DE, NH, NJ, NE, VT, TN, MD



Understand the Laws that Apply to Your Business

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





State Data Breach Reporting Statutes Specific to Tax Professionals

Virginia Code § 58.1-341.2

- Requires paid income tax return preparers to notify the Department of Taxation within a reasonable time period if they discover that an unauthorized person has accessed a taxpayer's return information.
- "Return information" means a taxpayer's identity and the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, assessments, or tax payments.

Idaho Code § 28-51-105(3)

- If the breach of computerized personal information involves an individual or commercial entity that prepares Idaho state tax returns and could possibly result in compromising any tax return or tax information [...] that individual or commercial entity shall give notice as prescribed by rule to the Idaho state tax commission as soon as possible, **but no later than five (5) business days**, after confirmation of the breach of security of the system



Practicing Cyber Hygiene



Mobile Devices and Apps

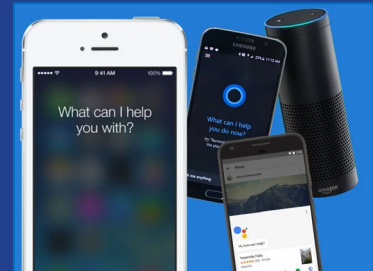
PRIVACY SETTINGS

➤ Location, microphone



IoT and Smart Home Devices

- Smart home devices listen for the “wake” word before recording
 - 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



Mitigating Telework-related Cyber Risks

- Distracted employees may be at higher risk of phishing
 - Engage in regular education and phishing tests
- Wi-Fi connections may be insecure
 - Use a secure Wi-fi and VPN connection
 - Use strong passwords for home routers and Wi-fi
- Household members may shoulder surf or use company devices
 - Use passwords for remote logins
 - Use multi-factor authentication



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.



MFA Fatigue Attacks



- An emerging form of social engineering
- First, the attacker needs the victim's login credentials
 - Typically, through a phishing email, a credential stuffing attack, or by purchasing them on the dark web
 - Once the attacker has obtained the victim's login credentials, they can attempt to log in to the victim's account or device, which has been secured with MFA.
- The attacker spams MFA requests with a frequency that is designed to overwhelm the victim's ability to properly verify the requests.
 - Timed to coincide with the target's routine log-ons



Risks of Portable Data Storage

- 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
- Risks with using USB storage:
 - Viruses and worms that specifically target USBs
 - Easy to lose/get stolen
 - Outside USBs may bring in viruses (never plug in an unknown USB device)



Cybersecurity Practices

1

Implement a process for addressing and fixing cybersecurity issues

2

Obtain adequate cybersecurity insurance

3

Implement a record retention policy

4

Conduct periodic independent audits

5

Implement least privilege and separation of duties

6

Implement multi-factor authentication





Vendor Management



Vendor Intake Survey

Ask about information security standards, practices and policies, and audit results

Look for recognized standards 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



Key Contractual Provisions

Look for contract provisions that give you the right to review audit results

Make sure that the contract requires ongoing compliance with cybersecurity and information security standards

Beware of contract provisions that limit the service provider's responsibility for IT security breaches

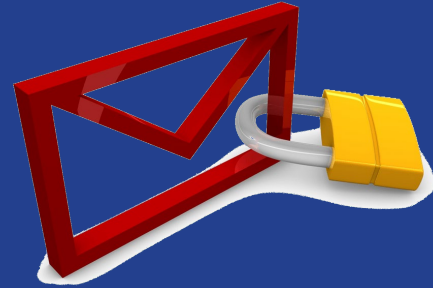
Manage Mobile Devices with a BYOD Program

Bring Your Own Device Program:

- Install and enable encryption, firewall, & remote wiping/disabling
- Disable/ do not use file sharing applications
- Use a complex password/passphrase or other user authentication (multi-factor authentication)
- Educate employees about mobile privacy, security awareness, and best practices



Secure Email Communication



- Enable encryption
- Verify Selected Recipients
- Use Standard Confidentiality Disclaimers
 - “Sensitive” communications should be given special protections against disclosure to third-parties
- 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
- Avoid email as a method for sending sensitive or confidential information
 - Use a secure document sharing platform if possible



Workplace Culture

- Cultivate a culture of privacy and security from the board room to the mail room and make cybersecurity training an on-going process
 - Make employees aware of the important role they play in privacy and security
 - Employees are your front line of defense, but also one of your highest risks



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





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



PELL CENTER

for INTERNATIONAL RELATIONS
and PUBLIC POLICY

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.