IRS Tax Forum | 2019

IRS Nationwide

Data Privacy and Cybersecurity for Tax Professionals

Robinson+Cole

CYBERSCOUT

Agenda

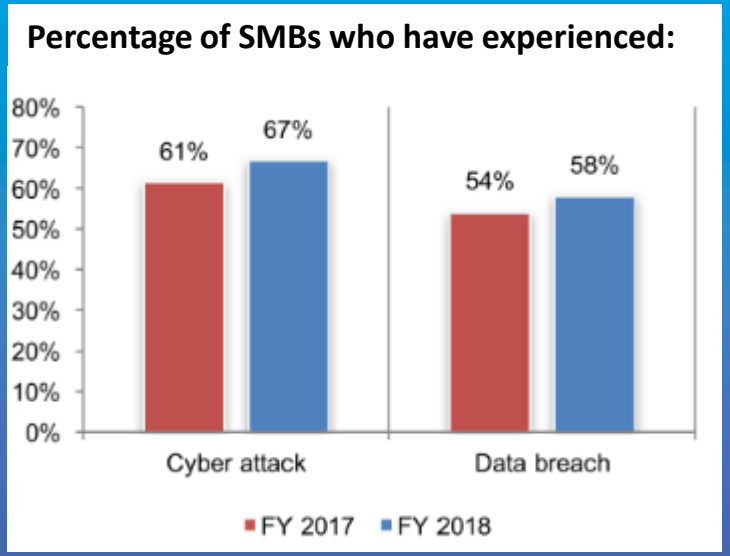
1. Identifying and Protecting High-Risk Data
2. Mapping Your High-Risk Data
3. Security Risk Assessments
4. What Laws Might Apply to You?
5. Enterprise-Wide Privacy + Security Program
6. Consider the Risks to Your Data
7. Best Practices

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.

Customer Data Makes You a Prime Cyber Target!

- The percentage of SMBs that experienced a cyber attack climbed from 61% to 67% in 2018.
- More than 60% of SMBs said the cause of the incident was a negligent employee or contractor.
- The average cost of cyber attacks on SMBs was more than 2.9 million in 2018 (up from $2.2M the previous year), with an average cost due to damage or theft of IT assets of over $1.4M, and an average cost for disruption to business operations reaching more than $1.5M.
- An estimated 60% of SMBs will go out of business within 6 months of a cyber attack.



2018 State of Cybersecurity in Small & Medium Sized Business (SMB)
Ponemon Institute, 2018

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
- 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.

IRS Tax Forum | 2019

IRS Nationwide

YOUR PII CHART™

Take time to inventory the identity relationships you have with the companies, organizations, and individuals you entrust with your personally identifiable information or PII. See how your identity is a PII Chart™, a picture of relationships you've created. Once you visualize the slices of your PII, managing your identity assets becomes easier.

LEGEND

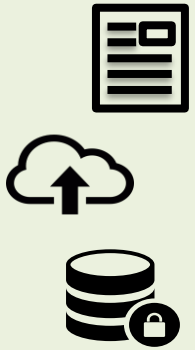
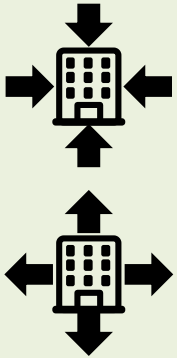
- **SOCIAL SECURITY NUMBER**
- **CONTACT INFORMATION** (email address, physical address, telephone and mobile numbers)
- **GOVERNMENT-ISSUED IDENTIFICATION** (driver's license, passport, birth certificate, library card)
- **BIRTH DATE, BIRTH PLACE**
- **ONLINE INFORMATION** (Facebook, social media, passwords, PINs)
- **GEOLOCATION** (smartphone, GPS, camera)
- **VERIFICATION DATA** (mother's maiden name, pets' and kids' names, high school, passwords)
- **MEDICAL RECORDS INFORMATION** (prescriptions, medical records, exams, images)
- **ACCOUNT NUMBERS** (bank, insurance, investments, credit cards)

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

STEP 2: Map Your High-Risk Data

- Determine where your high risk data is, 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

- IRS Regulations.
- State Data Breach Notification Law(s).

IRC Regulations

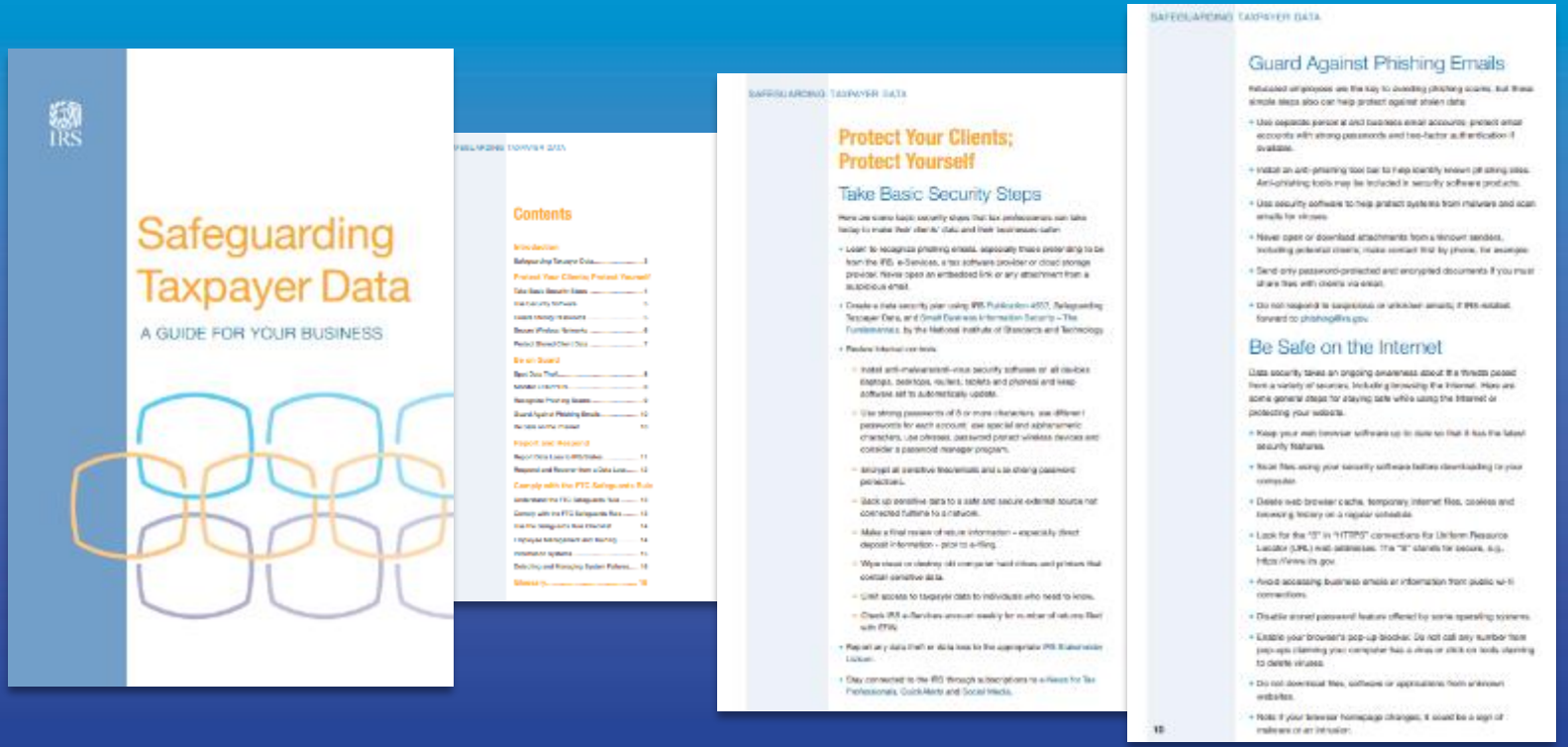
- Section 7216 of the Internal Revenue Code (IRC) imposes criminal penalties on tax preparers who make unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return.

- IRC Section 6713 imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.

IRS Guidance and Fact Sheets

FS-2015-24, October 2015

- The IRS recommends that preparers create a data security plan, using the IRS Publication 4557 on "Safeguarding Taxpayer Data."



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

- MINIMIZE the risks of an attack
- MONITOR for dangers
- MANAGE the damage

MINIMIZE: Enterprise-Wide Privacy + Security Program

- Policies, procedures and standards;
- Education through training and awareness;
- 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 & Procedures, and Security Policy & Procedures.

MINIMIZE:
Privacy & Security Policies, Procedures and Standards

- Acceptable Use Procedure;
- Social Media Standards and Guidelines;
- Bring Your Own Device Program;
- E-mail Procedure;
- Data Retention Program and Retention Schedule;
- HIPAA Compliance
  - If self-funded health plan.

MONITOR: Consider the Risks to Your Data

Cyber Attacks

- It could be anyone!
- If you throw a dart at a map of the world, you are likely to hit a source of the problem.
- Experts say the risk from attacks extends beyond losing information to opening opportunities for serious damage.
- With proper systems you CAN know where every attack is originating and how frequently. Do you?

Cyber Attacks: How does this happen?

- Through your network
  - Vulnerabilities in your hardware, software or systems.
  - Your employees and mistakes they might make.
  - Your clients, if, and to the extent they have access to your network.
  - Vendors and contractors, if and to the extent they have access to your network.

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.

MONITOR: Consider the Risks to Your Data

Phishing/Spear-Phishing

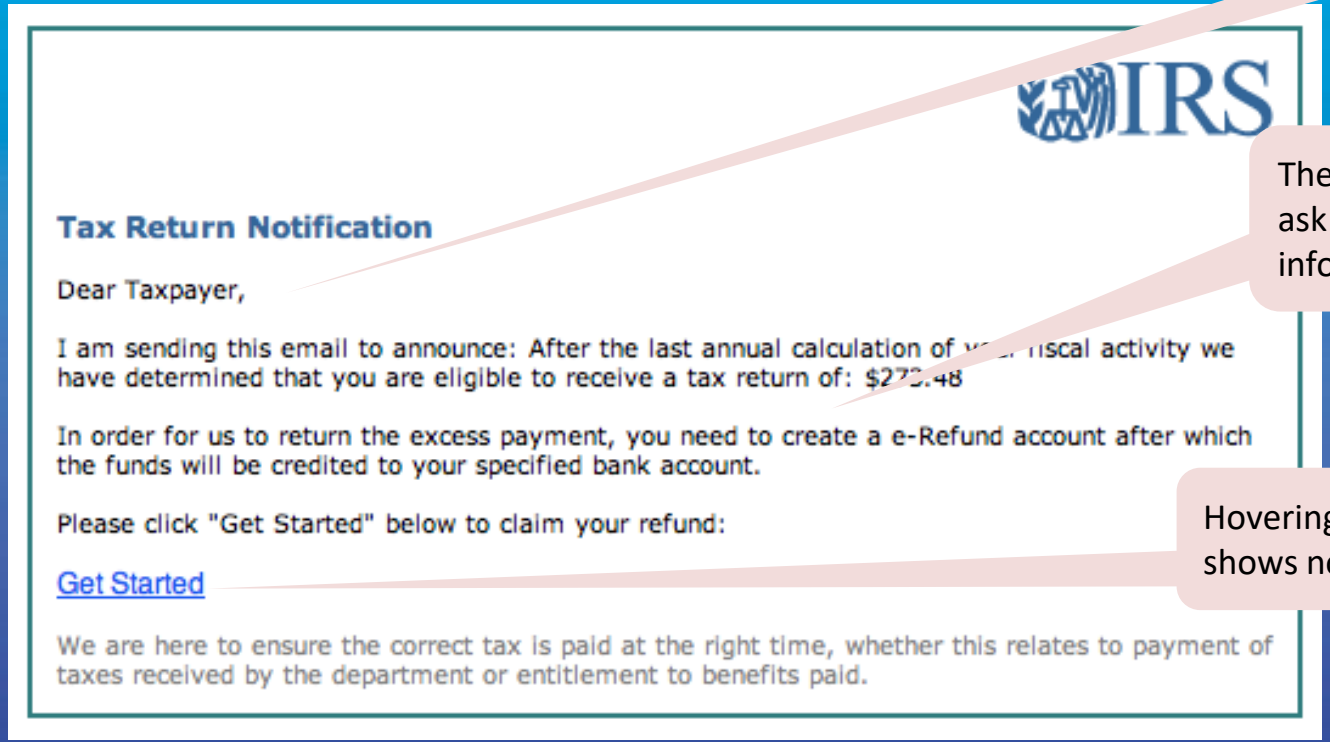
- IRS Issued Warnings to Payroll/HR Departments
  - March 1, 2016, February 2, 2017, March 4, 2019
  - Warning of phishing schemes that affected numerous companies
    - Phishing emails posing as state accounting or professional associations.
  - According to the IRS, "If your CEO appears to be emailing you for company employees' personal information, including SSNs, check it out before you respond."
  - If you receive suspicious emails related to taxes or the IRS, or phishing attempts to gain access to your databases, forward/report those emails to phishing@irs.gov.

MONITOR: Consider the Risks to Your Data

Phishing/Spear-Phishing

- FBI continues to warn businesses due to the "dramatic rise" in these schemes.
- Received complaints from victims in every state in the U.S. and at least 100 countries, from 22,143 victims.
- To date, the losses associated with email scams total more than $3.1 billion.

Phishing



Generic Greeting

The IRS would never ask for this kind of information via email

Hovering over the link shows non-IRS site

Spear Phishing

From: Daniel Rais
Sent: Wednesday, January 25, 2017 3:00 a.m.
To: francesca.spidalieri@salve.edu
Subject: Great conference speech!

Hi Francesca,

I very much enjoyed your recent presentation at the cybersecurity conference and wanted to share with you an interesting article on the same subject, http://www.fordes.com/sites/2017/01/02/cybersecurity&riskmanagement/#1e797d807d27

I look forward to meeting you again in the future.

Best Regards,

Daniel Rais

From: Help Desk
Sent: Monday, August 4, 2016 8:00 a.m.
To: Joe@mycompany.com
Subject: System Access Update

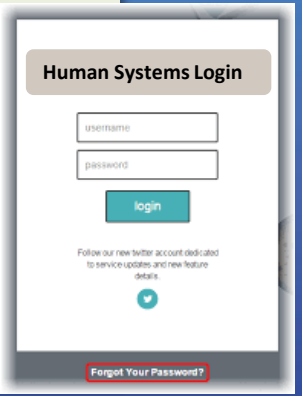
Dear Joe,

Our records indicate you have not changed your password in the last 90 days. If you do not change your password within the next 24 hours, your access to Human Systems will be suspended.

To access Human Systems, follow the link below:
HTTPS://human-systems-access.mycompany.com/password update

As a reminder:
- use complex passwords
- Change passwords every 90 days
- Do not use passwords that you use on other sites

Sincerely,
Help Desk



IRS Tax Forum IRS Nationwide 2019

PELL CENTER for INTERNATIONAL RELATIONS and PUBLIC POLICY

If you receive a phishing email

- **Be aware** – Be wary of any urgent or confidential requests.
- **Think before replying** – Never "reply" to the email containing a suspicious request.
- **Authenticate the sender** of the message by contacting him/her by an alternative method
- **Confirm twice**– Contact a different person at the company with whom you have a relationship before authorizing transactions.
- **Check your sent mail, junk mail, and email account settings regularly**– Hackers often break into an email account and modify the "email forwarding" settings to forward emails to their own account.
- **Don't email sensitive or confidential information** – Consider using a secure document sharing or transaction management platform.
- **Regularly purge** your email of unneeded or outdated information – Save any important emails securely.
- **Alert your bank** of any potentially fraudulent transaction.
- **Educate your family members and your employees** about the potential impact of online scams.
- **Create a process** for employees to report phishing incidents.
- **Remove or quarantine** infected machines.

Ransomware

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

- 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.

For consideration

- Don’t click on unknown links;
- Keep your anti-virus software up to date;
- Back up all sensitive information;
- Employee education.

MONITOR: Consider the Risks to Your Data

Ransomware/Malware

- IBM Security released a report in 2017:
  - 70% of companies infected with ransomware pay ransom to get the decryption key for access to data.
  - Half of the 1,621 companies surveyed said they had been attacked with ransomware.
  - Of the 70% who paid, more than half paid more than $10,000 for the decryption key, while 20% paid more than $40,000.
- 60% of executives said they would pay to recover their data and 25% of them said they would pay between $20,000 and $50,000 to recover customer records, financial information, intellectual property and business plans.
- Based upon the survey, it does not appear that ransomware is going away any time soon!
- The profit margins and incentives are high for cyber criminals to continue attacking businesses with ransomware.

MANAGE: Develop an Incident Response Plan

- Incident Response and Breach Notification Plan
  - To be effective, the incident response plan and breach notification process must be part of a comprehensive information security plan:
    - Risk assessment
    - Trigger events
    - Mitigation plan
  - Identify State and Federal Laws and Requirements
  - Communications/Media Team/Vendors in Place
  - Breach Notification Laws Across the Country
    - 50 State Breach Notification Laws
- 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 (and 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.

Case Study from 2018

- A tax accountancy firm in New York was informed several clients had filed suspicious returns
- CyberScout determined no active exploitation of the company's network or direct system compromise.
- CyberScout then conducted passive and deep web discovery of their partners and service providers.
- Breach discovered with Disaster Recovery Provider resulting in compromise of almost all of accounting firm's data
- Ransomware and exfiltration of taxpayer data had occurred.
- CyberScout analyzed data and determined PII at risk so accounting firm could notify clients.

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

MINIMIZE

MONITOR

MANAGE

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.

- If a mobile device contains personal information and the personal 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 secure it could be a reportable data breach.

Best Practices with 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;
- 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 or other user 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.

IRS Tax Forum | IRS Nationwide | 2019

Actions Clients and Tax Preparers can Take to Protect Themselves

Best Practices for Transportation of Data

- **Use a chain of custody log:** Tracking data, times and dates of transfers, names and signatures of individuals releasing the information, and 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.

Best Practices 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.

Best Practices when Using E-mail

- Encryption;
- Virtual Private Network/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."

Best Practices to Protect Paper Records

Protect High risk data

- Any documents with SSN
- W-2s
- Health insurance records
- Benefits records
- Salary and personnel information

How to Protect

- Lock filing cabinets
- Lock offices/building/rooms
- Only accessed by authorized personnel with a need to know
- Do not send via regular mail
- Implement a Retention Program
- Destroy any paper records that don’t need to be kept/stored

IRS Tax Forum | IRS Nationwide | 2019

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
- **US-CERT**
  - www.us-cert.gov
- **InfraGard**
  - www.infragard.org
- **SANS Institute**
  - www.sans.org

IRS Tax Forum | 2019

IRS Nationwide

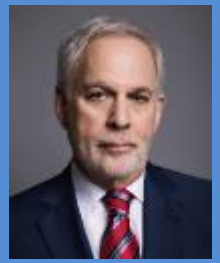
AMERICAN COALITION FOR TAXPAYER RIGHTS

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

Thank You / Questions

Matt Cullina
Managing Director, Global Markets
CyberScout
Email: alevin@cyberscout.com

Our Mission
As trusted partners, we help your customers minimize, monitor and manage identity theft, fraud and cyber risk.



Adam Levin
Chairman & Founder
CyberScout
Email: alevin@cyberscout.com

Our Mission
As trusted partners, we help your customers minimize, monitor and manage identity theft, fraud and cyber risk.

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.

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.

IRS Tax Forum | 2019 IRS Nationwide

CYBERSCOUT

SALVE REGINA UNIVERSITY PELL CENTER for INTERNATIONAL RELATIONS and PUBLIC POLICY

Robinson+Cole