Cybersecurity Options for Your Apprenticeship Fund

Adam T. Boston, Esq.
Chief Legal Officer
Data Privacy Officer
International Painters and Allied Trades Industry (IUPAT) Pension Fund
Hanover, Maryland

Rebecca L. Rakoski, Esq.
Managing Partner
XPAN Law Partners LLC
Philadelphia, Pennsylvania

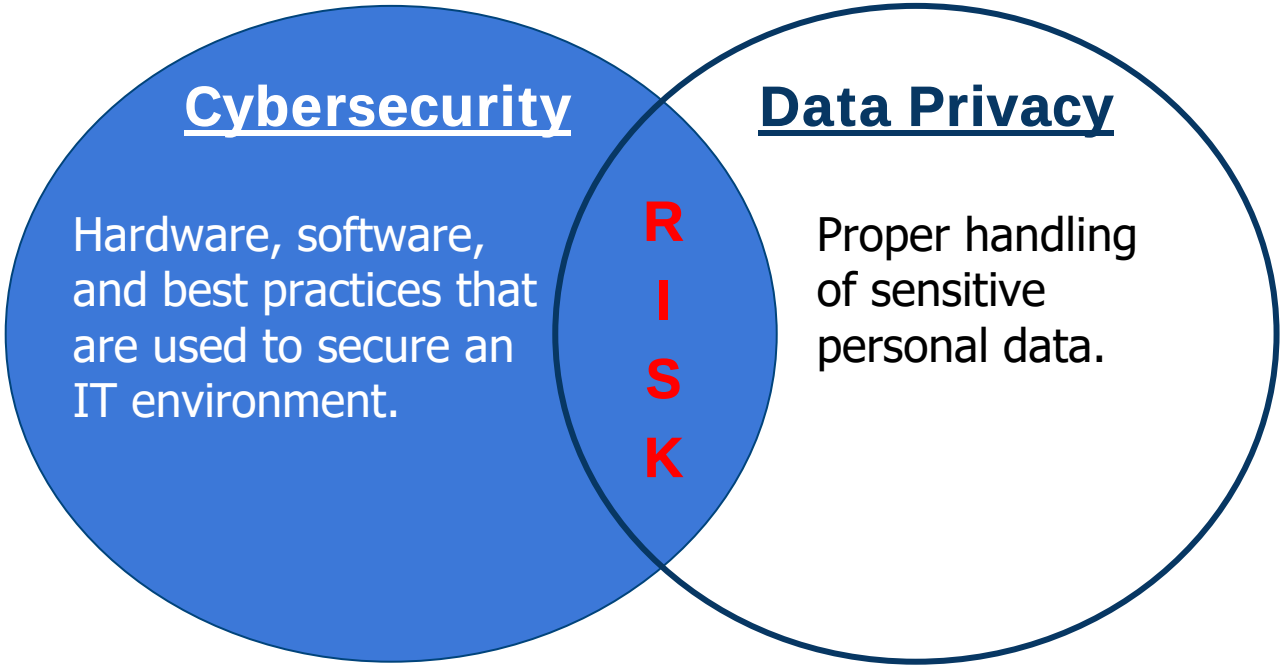
70TH ANNUAL EMPLOYEE BENEFITS CONFERENCE

International Foundation OF EMPLOYEE BENEFIT PLANS

Roadmap

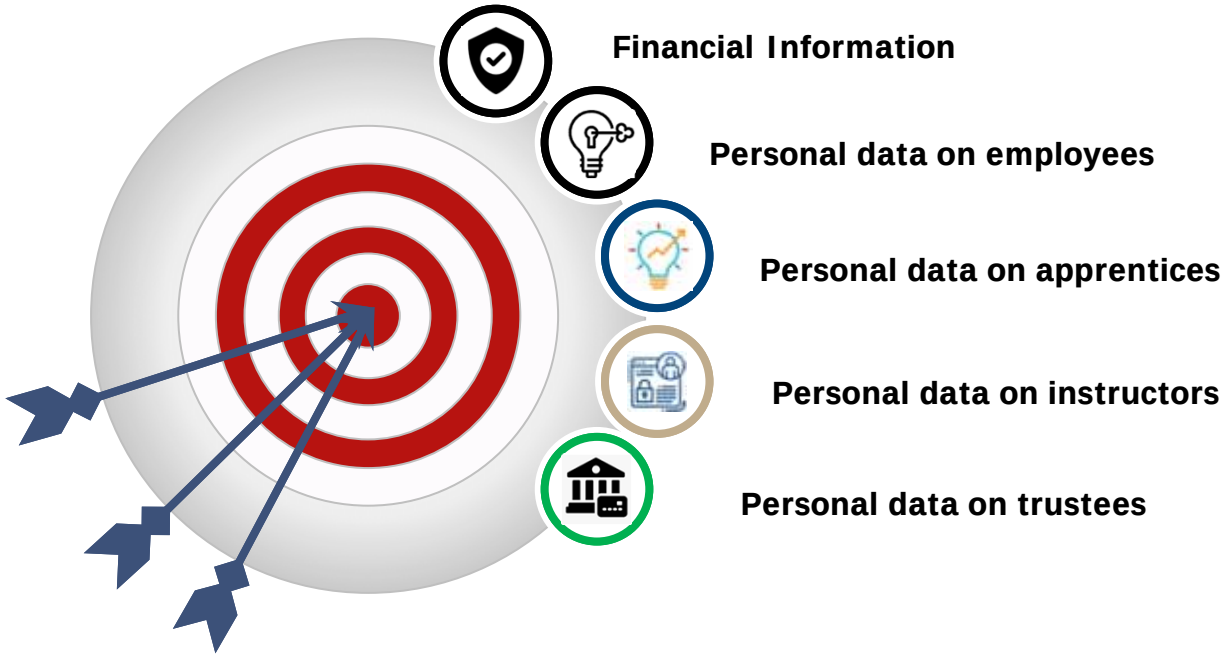
- Cybersecurity vs. data privacy
- Risks to apprenticeship funds
- Regulatory environment
  - DOL rules on cybersecurity
  - Regulatory requirements
  - Special consideration: FERPA
- Legal threats: Taking on the plaintiff's bar
- Tackling good governance
  - Setting a standard
  - Implementing and monitoring
- Additional materials

Cybersecurity vs. Data Privacy



Cybersecurity and Data Privacy Risks Specific to Apprenticeship Funds

Risk #1: The Data



Risk #2: Increased Use of Online Learning

Risk #3: Lack of Resources

- Lack of financial and technological resources for larger retirement and health plans
- No dedicated staff to manage IT
- Staff members who have access and control over data lack IT background and/or time
- Forced to rely on shared services agreements or expensive consultants

Risk #4: Lack of Appropriate Policies, Training and Education

- Policies are adopted or boilerplate, not tailored, implemented or appropriately monitored
- Lack of education or phishing training
- Lack of training and education on tailored cyber/privacy programs
- General knowledge → Not specific to Fund!

Risk # 5: Severe Operational and Financial Impact

- Unable to operate
- Financial ruin/distress
- Unwanted redirection of needed educational resources

Why So Expensive?

- Forensic/technical investigation
- Legal
- Public relations
- Notification
- Regulatory fines/penalties
- Regulatory investigations
- Lawsuits

Why So Severe…Investigations

Understanding the Role of Insurance

- First-party coverage
- Third-party coverage
- Wire fraud claims
- Insurance limits and claims management
- Insurance is not a cure-all

Regulatory and Legal Requirements

DOL Guidelines

- Applies to plan sponsors, **plan fiduciaries**, record keepers and plan participants on best practices for maintaining cybersecurity.
- Directed at plan sponsors and **fiduciaries** regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries.
- Goal is to protect the retirement benefits of America's workers. (***THIS MEANS MEMBERS COME FIRST)***

Updated guidance released

September 2024

ERISA

- ERISA requires plan fiduciaries to act with the "care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use."
  ERISA § 404(a)(1)(B)
  (29 U.S.C. § 1104(a)(1)(B))

- When applying ERISA's prudence requirement, courts and the Department of Labor (DOL) generally focus on whether the fiduciary followed a *good process*.

Fiduciary Obligation

- Duty of Prudence
  - Fiduciaries must act prudently and solely in the interest of the plan, participants and beneficiaries.
    - Prudently develop policies and procedures to protect information that is handled, processed, collected, transmitted, and stored (not just PHI – PII and participant data too).
    - Prudently prepare for and respond to a breach scenario.
    - Third-party procedures (protect, notify, and remediate)

DOL Cybersecurity Guidance

- The guidance relates to three (3) main areas of focus:
  - Cybersecurity best practices
  - Online security tips
  - Third-party service providers

#1: Cybersecurity Best Practices

- Documented cyber program
- Annual risk assessment
- Annual third-party audit of security controls
- Clearly define security roles and responsibilities
- Access control procedures
- Appropriate security reviews and assessments of cloud storage providers

#1: Cybersecurity Best Practices

- Conduct cyber awareness training
- Implement and manage a security system development life cycle program
- Have a business resiliency program addressing business continuity, disaster recovery and incident response
- Encrypt sensitive data in transit and at rest
- Implement technical controls
- Respond to past cyber incidents

#2: Online Security Tips

- Register, set up and routinely monitor your online account
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Close or delete unused accounts
- Be wary of free wi-fi
- Beware of phishing attacks
- Use antivirus software and keep apps and software current
- Know how to report identity theft and cybersecurity incidents

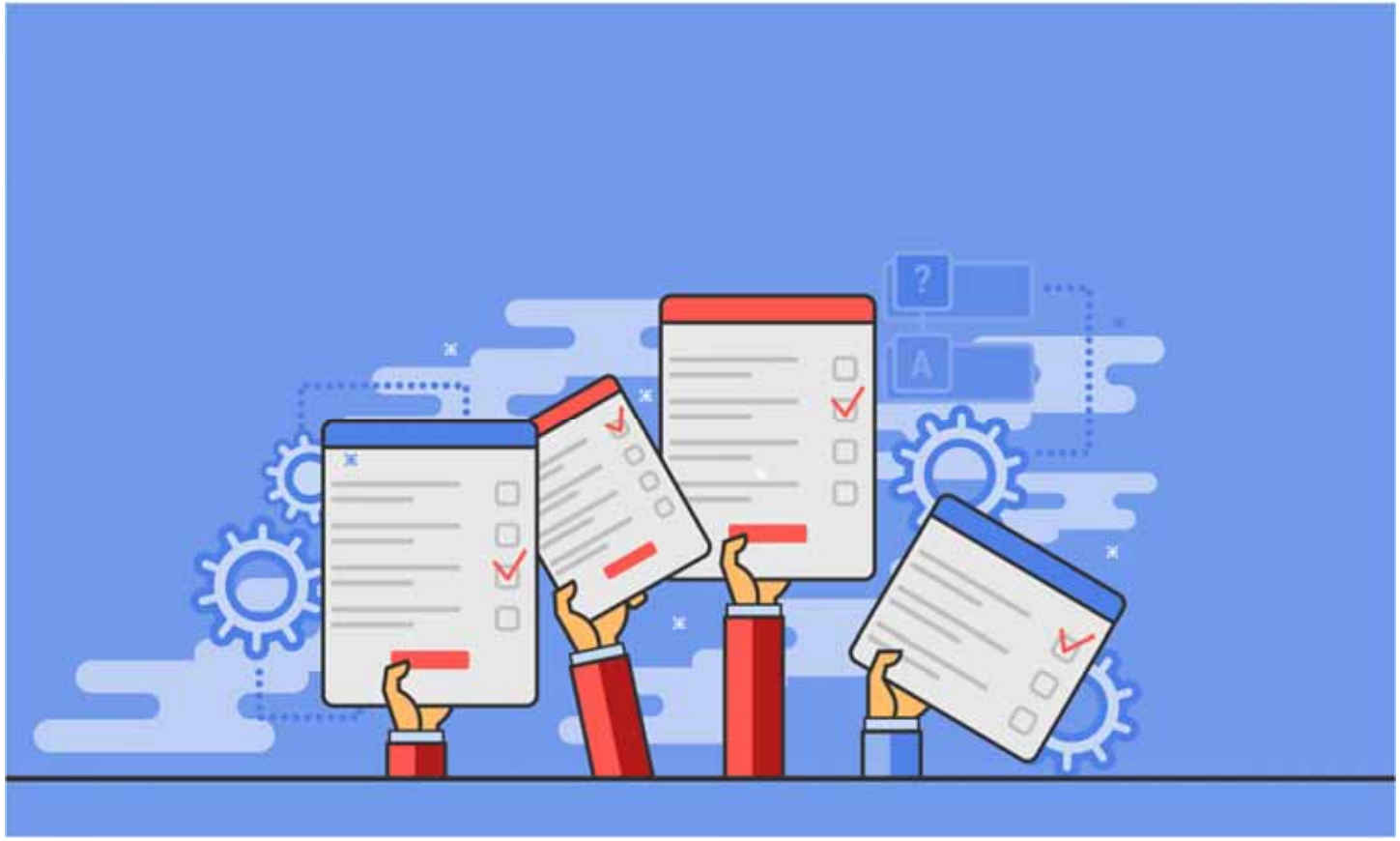
#3: Third Parties: DOL Requirements

- Ask about security standards, practices and policies, and audit results
- Ask the service provider how it validates its practices
- Evaluate the service provider's track record in the industry
- Ask about past security breaches
- Does service provider have insurance policies?
- Create contract language around requirements

Sample Audit Questions: Third Parties

- All documents constituting or reflecting any security reviews and/or **independent security assessments** performed that relate to assets or data stored in a cloud or managed by a **third-party service provider**.
- All documents constituting or relating to any **contracts** with any third-party service providers that provide services relating to the plan's information security, cybersecurity or security controls.

Questionnaires



Legal Threats:
Taking on the Plaintiff's Bar

Where Victims Become Defendants

Where Victims Become Defendants...

- Breach of fiduciary duty
- Breach of contract
- Breach of implied contract
- Negligence
- Negligence per se
- State consumer fraud statutes
- Third-party indemnification

Keown v. International Association of Sheet Metal Air Rail Transportation Workers

- Background
  - Former union members' putative class action stemming from a cyberattack that compromised the members' personal information.
  - The former members plead common law breach of implied contract claims and common law negligence claim
  - Claims that:
    - Data breaches are preventable
    - Defendant acquires, collects and stores plaintiff's and the class's PII defendant knew, or should have known, the risk of the risk because labor unions in possession of PII are particularly susceptible to cyber attacks
    - PII is valuable
    - Defendants failed to comply with FTC guidelines
    - Defendants failed to comply with industry standards

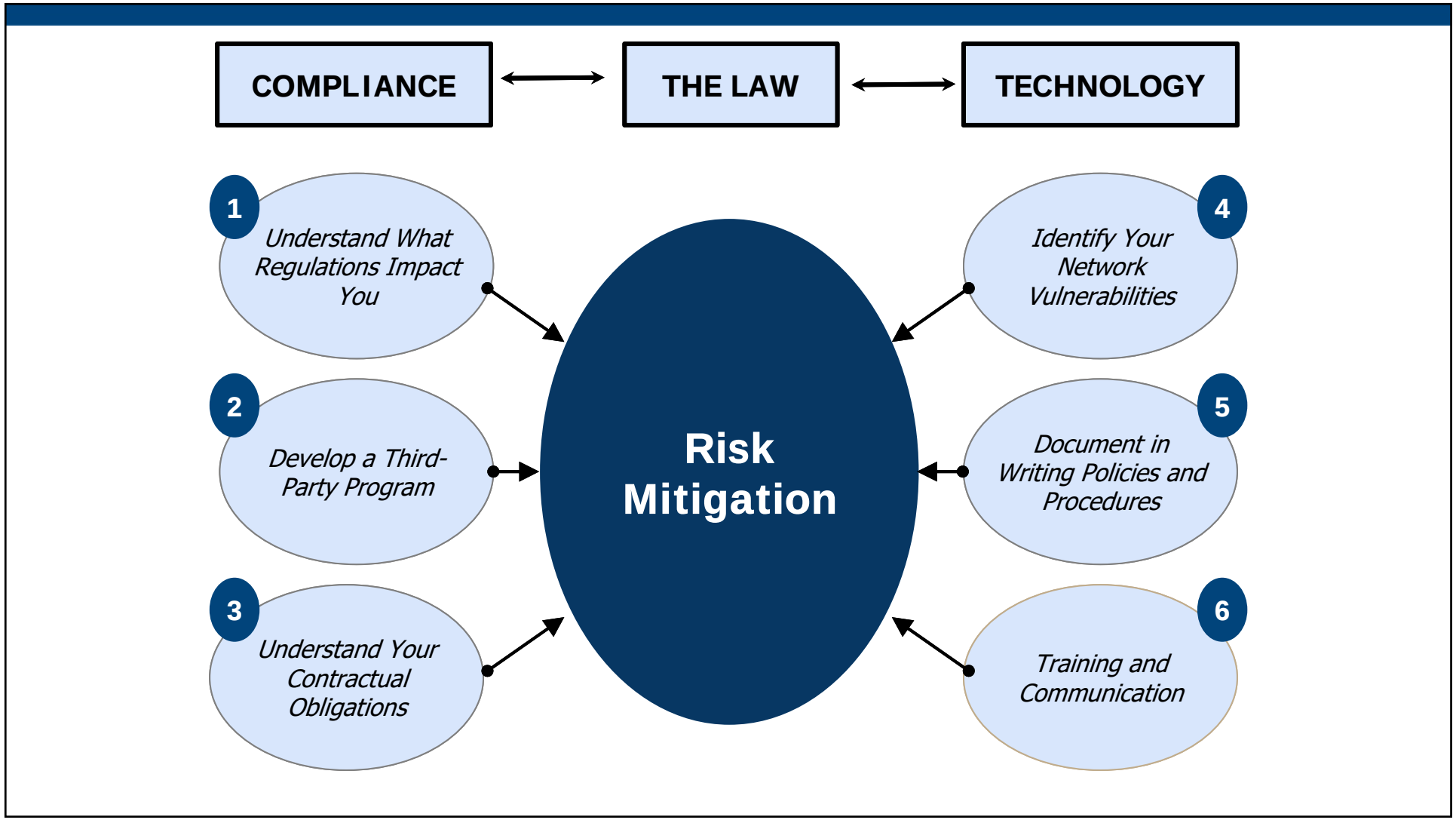
Keown v. International Association of Sheet Metal Air Rail Transportation Workers

32. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its union members' PII safe and confidential.

33. Defendant had obligations created by the **FTC Act**, contract, industry standards and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

Risk Mitigation Strategies

- Make a roadmap and stick to it!
- Share resources where appropriate.
- Demand the 3Ts (talent, treasure, time)
- Own your own governance.
- Stop using just “tech” solutions
- Review, rinse, repeat!

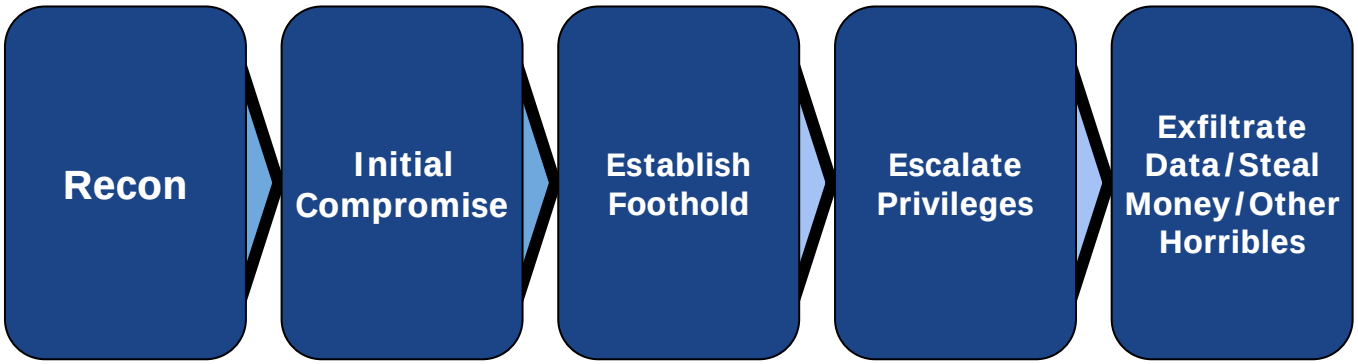

COMPLIANCE
THE LAW
TECHNOLOGY
1
Understand What Regulations Impact You
2
Develop a Third-Party Program
3
Understand Your Contractual Obligations
Risk Mitigation
4
Identify Your Network Vulnerabilities
5
Document in Writing Policies and Procedures
6
Training and Communication

Your Feedback Is Important.
Please Scan This QR Code.

Session Evaluation

Additional Material and Information

How Hacking Works



Methods Used

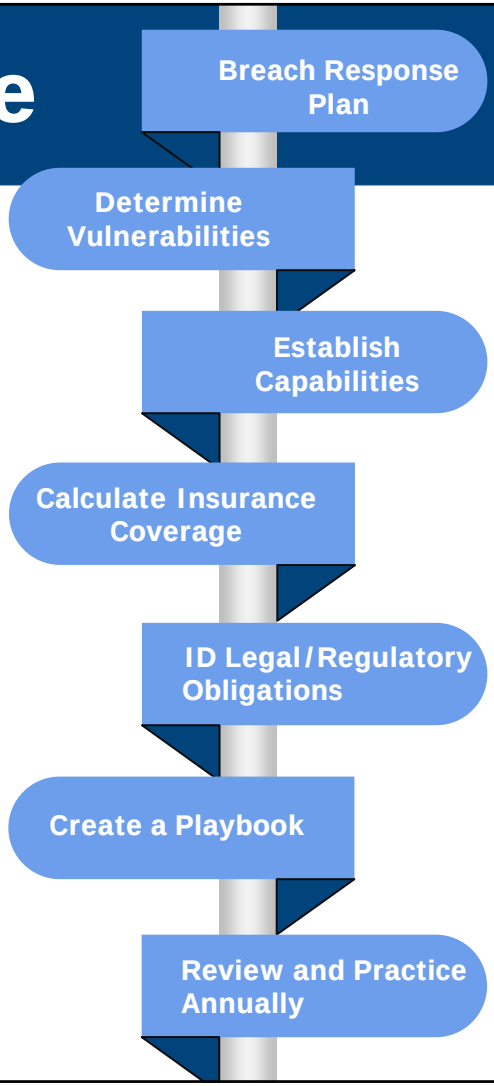
- Phishing
- Spear phishing
- Deep fake
- Ransomware
- Malware
- Fraud transfers

Dealing With a Data Breach

Data Breach Notification Laws

- What constitutes a data breach?
- Personal information?
- Notification obligations?
- Reporting obligations?
- Third-party notifications?
- Timing of notifications?
- Good faith exception?

Data Breach Response



Business Resiliency Program / Breach Response Plan

- Create a team and contact lists
- Identifying important/critical services
- Maintain a centralized list of important/critical services and processes
- Determine needs to maintain important/critical services during a disaster
- Determine and formulate how each department will continue to perform critical functions and preserve critical
- Identify key resources and interdependencies across department groups
- Maintain and update applicable documentation (including technical business documentation; list of high-value assets High Value Assets (HVA) list; list of high-value data (See SP-03.00, Data Inventory/Classification Policy); Business Operations Documentation; Up to date IR Plan; and validated and updated contact lists)

Example: Security Team Tasks

- **Task 1:** Coordinating with third-party service providers
- **Task 2:** Ascertain size and scope of security incident
- **Task 3:** Maintain documentation and confidentiality
- **Task 4:** Ensure legal's role throughout implementation of plan