MINTZ

Cybersecurity and Employee Benefit Plans: Where Are We Now?

Worldwide Employee Benefits Network

December 13, 2023

Segment II Presented by:

Michelle Capezza
Of Counsel, Mintz
MCapezza@mintz.com
212.692.6815

Cybersecurity Risks

Organizations are vulnerable to cybersecurity risks, including:

- System vulnerabilities
- Software/hardware vulnerabilities/inadequate patch management
- Ransomware attacks
- Endpoint attacks
- Phishing scams
- Cloud services
- Third party attacks
- Employee risks/remote work
- AI attacks, IoT attacks, formjacking, cryptojacking
- Lack of training/education/cybersecurity expertise

Cybersecurity Risks

Employee Benefit Plans are vulnerable to cybersecurity risks, including:

- Collection, transmission, storage, handling sensitive participant and beneficiary data
- Multiple service providers
- Electronic administration/Online accounts
- Cloud services
- Mobile account access
- Varieties of aps
- Digital asset investments
- Artificial Intelligence in benefits

Plan sponsors and fiduciaries have plan management responsibilities that are increasingly more complex. There is no comprehensive law governing cybersecurity for benefit plans.

ERISA Fiduciary Responsibilities and Liability

Who are the ERISA plan fiduciaries?

What are the fiduciary responsibilities under ERISA?

Who can bring fiduciary breach claims under ERISA?

Are there potential fiduciary breach claims related to participant data and cybersecurity of benefit plans?

What is the current landscape of laws that affect data privacy and security?

EBSA (DOL) focus on cybsersecurity in the context of benefit plans and audits

ERISA Plan Fiduciaries Include Individuals or Entities who:

Exercise any discretionary authority or control over the management of the plan or management or disposition of plan assets

Render investment advice to the plan for a fee

Have discretionary authority or responsibility in plan administration

Fiduciaries are “named” in the plan documents and other individuals can be fiduciaries based on their functions

ERISA Plan Fiduciary Responsibilities

Act solely in the interest of plan participants and beneficiaries (duty of undivided loyalty)

Act with exclusive purpose of providing plan benefits and defraying reasonable expenses of administering the plan (exclusive benefit rule)

Carry out duties with care, skill, prudence and diligence (prudent person rule)

Diversify plan investments to minimize risk of large losses (diversification rule)

Follow plan document terms (unless inconsistent with ERISA), interpreting provisions, maintaining plan documents

ERISA Advisory Council Reports and DOL Guidance

- Reports prior to DOL/EBSA guidance
  - Privacy and Security Issues Affecting Employee Benefit Plans (November 2011)
  - Cybersecurity Considerations for Benefit Plans (November 2016)
- The April 14, 2021 DOL/EBSA Guidance—fiduciary responsibility to mitigate cybersecurity risk
- Reports after the DOL/EBSA Guidance
  - Cybersecurity Issues Affecting Health Benefit Plans (December 2022)
  - Cybersecurity Insurance and Employee Benefit Plans (December 2022)
- “8 Tips for Protecting Your Retirement Savings Online”-June 26, 2023

DOL/EBSA April 14, 2021 Guidance on Cybersecurity Best Practices

Cybersecurity Program Best Practices

Tips for Hiring a Service Provider

Online Security Tips for Plan Participants

DOL/EBSA April 14, 2021 Guidance

"To help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips…"

See TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES Guidance

DOL/EBSA April 14, 2021 Guidance

“Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.”

See CYBERSECURITY PROGRAM BEST PRACTICES Guidance

Fiduciary Responsibility to Mitigate Risk

Examples of plan fiduciary considerations:

- Develop cybersecurity policies and procedures for mitigating cybersecurity risk
- Identify the data and information collected, processed, transmitted and stored
- Be prudent in selecting and monitoring service providers
- Address cybersecurity protections in service agreements
- Cyberinsurance and other insurance/risk mitigation strategies
- Coordinate data protection and cybersecurity breach response with organizational protocols
- Status of employee training
- Educate participants

Be prepared for a plan cybersecurity audit, claim, complaint, or breach response.

December 2022 ERISA Advisory Council Reports

- **Cybersecurity Issues Affecting Health Benefit Plans (December 2022)**
  - Cybersecurity policies and procedures for all employee benefit plans, not just retirement plans

- **Cybersecurity Insurance and Employee Benefit Plans (December 2022)**
  - Holistic review of insurance and risk mitigation strategies, as well as insurance coverage education for plan fiduciaries

Examples of Potential Claims

- ERISA Section 502(a)(2)
- ERISA Section 502(a)(3)
- ERISA Section 502(a)(1)(B)
- State Law Claims
- ERISA Preemption
- Patchwork of Privacy and Security Laws

Are You Audit Ready? Sample Inquiries

- Criteria used to select the service provider
- Plan sponsor and service provider cybersecurity and information security program policies, procedures, and guidelines that relate to the plan
- Data governance, classification, disposal
- Encryption to protect all sensitive information transmitted, stored, or in transit
- Implementation of access controls and identity management, including any use of multi-factor authentication
- Processes for business continuity, disaster recovery, and incident response
- Management of vendors and third party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties
- Data breach response procedures
- Cybersecurity awareness training

Are You Audit Ready? Sample Inquiries

- All documents and communications relating to any past cybersecurity incidents
- All security risk assessment reports, security control audit reports, audit files, penetration test reports and supporting documents, and any other third party cybersecurity analyses
- All documents and communications describing security reviews and independent security assessments of the assets or data of the plan stored in a cloud or managed by service providers
- All documents describing any secure system development life cycle (SDLC) program, including penetration testing, code review, and architecture analysis
- All documents describing security technical controls, including firewalls, antivirus software, and data backup
- All documents, service agreements, and communications describing the permitted uses of data by the sponsor of the plan or by any service providers of the plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services
- All documents demonstrating fiduciary oversight (e.g., Meeting Minutes)

Tarter Krinsky & Drogin

Celebrating 40 years our anniversary WEB Worldwide Employee Benefits Network

Cybersecurity and Employee Benefit Plans: Where are we now?

Amy B. Goldsmith, Esq.

Co-Chair, Cybersecurity, Data Management & Privacy Practice

Image by alan9187 from Pixabay

STATISTICS

3 seconds to encrypt

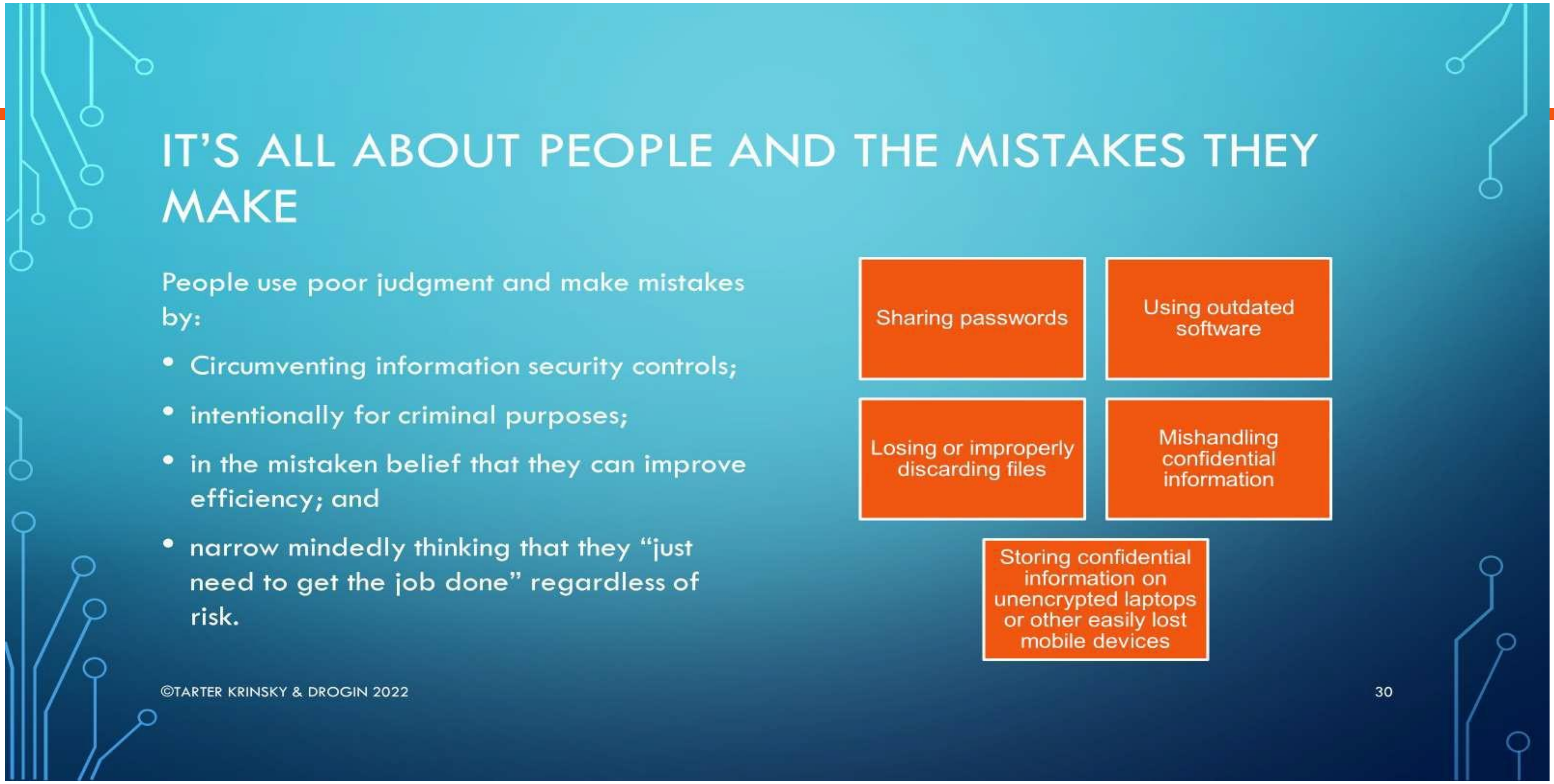
Attacks every 11 seconds

Ransomware = 2023

Average payment: $1.54 million

Total Average Cost: $4.54 million

"Do we really need to encrypt our data? Most of our communications are impossible to understand in the first place."



IT'S ALL ABOUT PEOPLE AND THE MISTAKES THEY MAKE

People use poor judgment and make mistakes by:

- Circumventing information security controls;
- intentionally for criminal purposes;
- in the mistaken belief that they can improve efficiency; and
- narrow mindedly thinking that they "just need to get the job done" regardless of risk.

Sharing passwords

Using outdated software

Losing or improperly discarding files

Mishandling confidential information

Storing confidential information on unencrypted laptops or other easily lost mobile devices

Ransomware

LOCKER

The device is locked

Ransom must be paid to unlock the device

Ransom messages may mimic law enforcement

Hackers may release embarrassing content

Data is not destroyed and may be able to be retrieved

CRYPTO

Access to files is locked, not access to the device

Data cannot be read without the hacker’s decryption key

Ransom messages say “Give me money, I’ll give you the key”

So how does hacking happen?

Unsecured Communications

1. Are your communications unencrypted? (public WiFi)
2. Are your smart devices (phones, webcams, modems, routers) unsecured?
3. Are your passwords following the KISS principle?
4. Is the software you use continuously updated?

You've Been Invaded

- Remote Access Trojan malware enables spying on users, reach messages, take screenshots, hijack webcams
- Connecting to unsecured networks creates an open road for a hacker

Understanding Malware and End User Attacks

Data theft

Attacks from the inside

DoS and DDoS attacks

Advanced persistent threats

Malware

Data Theft

Wiretaps: IoT devices, including Alexa and Google, are vulnerable

Domain Name Hijacking: without permission, the ownership or administration of a domain name is changed

Spoofing: an email is sent from a false sender address which may mimic an internal company address; it could contain a link to malware

Phishing: emails that look like they are from reputable companies; it could contain a link to malware

Dark web: company data is already compromised and available for sale on the dark web

"Technically, a screensaver saying
'no trespassing' isn't a firewall."

Social Engineering

Phishing, spear phishing, spoofing, robocalling, baiting, pre-texting: 50% of all breaches, text messaging

- Goals:
  - The hacker wants personally identifiable information such as names, license and social security numbers, financial account information; credit cards, tax forms of employees
  - The hacker wants usernames, passwords, and any other credential
  - The hacker wants information about the IT systems, data, and networks
  - The hacker wants money wired

Being Cyber Aware and Cyber Secure

Prevention, Detection and Response

Authentication to access system remotely

b) Update browser and web server software; be aware of all Microsoft and Apple vulnerabilities

c) Robust protocols for all transactions for disclosing sensitive data and making payments; double authentication, review and approval

Being Cyber Aware and Cyber Secure

Registration of like-kind domain names

Implementation of cybersecurity measures

Periodic Drills and Training

My gosh!

- **Best Practices**
  - Software updates and patches continuously
  - Train your people to use unique passwords for different accounts
  - USE HTTPS ENCRYPTION: https://www.tarterkrinsky.com
  - Don’t click on strange links or pop-up ads
  - Router and smart devices: create a new username and password, don’t use the ones that were assigned

And there’s more!

- Downloads should only be from trusted businesses; consider having it in control of all downloads
- Install anti-virus software on all systems, including personal laptops and phones
- Use a virtual private network
- Do not use ‘admin’ as a default for your IT department
- Assign strong passwords to employees; use a password manager
- Authentication: 2 factor (pushing a code to a phone, for instance)

We’re not done…

- Firewalls/Security Controls/End Point Detection/Segmentation
- Data Mapping/Hardware Inventory/Software and Application Inventory
- Regular Patching Schedule
- Encryption
- Training
- Cybersecurity Risk Heat Mapping

Monitoring

Company has the right to monitor the employee’s use of the company’s network and systems and personal phone if it is being used by the employee to access the company

No expectation of privacy when an employee uses the company’s network or systems

What do you need to write?

- Written Information Security Program
- Cyber and Information Security Policy
- Incident Response Plan
- Business Continuity Plan
- Vendor Contract Management Plan

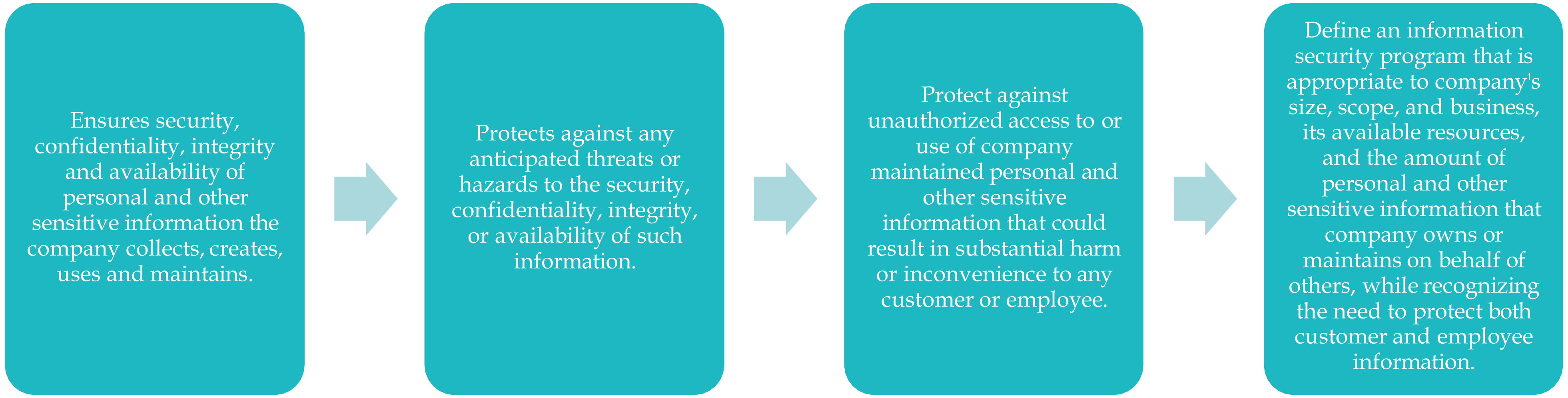
Goals

(1) Protect the security and confidentiality of the information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

WISP



Ensures security, confidentiality, integrity and availability of personal and other sensitive information the company collects, creates, uses and maintains.

Protects against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

Protect against unauthorized access to or use of company maintained personal and other sensitive information that could result in substantial harm or inconvenience to any customer or employee.

Define an information security program that is appropriate to company's size, scope, and business, its available resources, and the amount of personal and other sensitive information that company owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

What information is being collected?

Name

Residence Address

Citizenship

Identifiers (social security, license)

Mobile Number

Personal Financial Information

Accountability

INFORMATION SECURITY COORDINATOR

Initial implementation of WISP and other documents

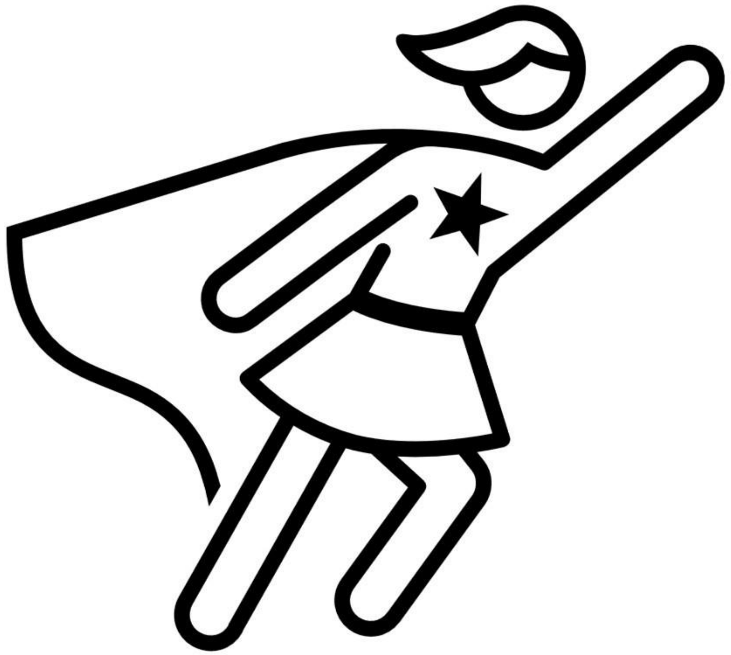
Risk assessment

Develop, design, distribute and maintain information security

Oversight of internal/external IT and Cyber

Monitor, test and train

Incident response plan



Cyber and Information Security Policy

Outlines how the personal information and sensitive information is protected

States that employees have no expectation of privacy and explains monitoring

Lists applicable regulations particular to the company's business

Explains Data Information Classification and Risk Based Controls

Incident Response Plan

(a) Define the Company’s cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist the Company and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.

(c) Mitigate or minimize the effects of any information security incident on the Company, its clients, employees, and others.

Incident Response Plan

(d) Help the Company consistently document the actions it takes in response to information security incidents.

(e) Reduce overall risk exposure for the Company.

(f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in the Company's information security program and incident response process.

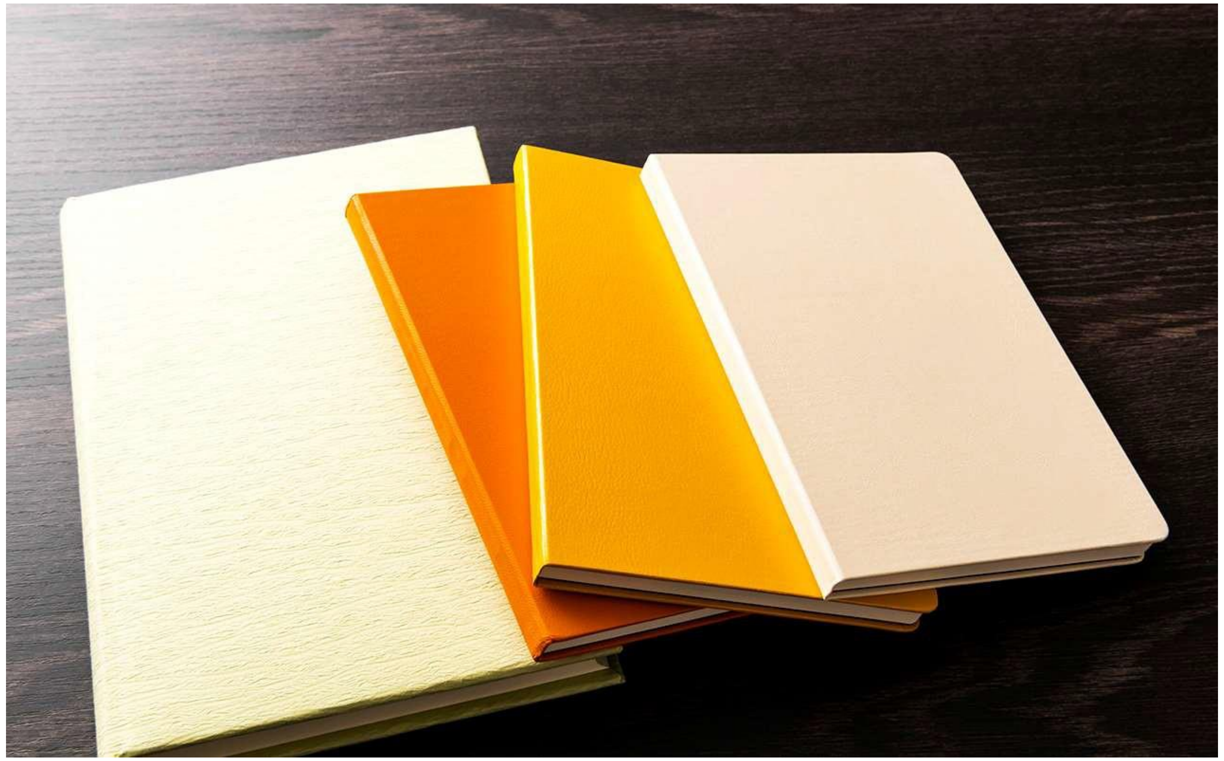
IRP Checklist

Who are the members of the Incident Response Team?

Who are your outside resources?

Where is the summary of your data collection and retention practices?

Who is responsible for preservation? Communication?



Breach Coach

Is your attorney your "Breach Coach"?

Selection and monitoring of Forensic Providers

Data Breach Reporting analysis and drafting

Contractually Obligated Data Breach Reporting

Mitigation of Damages

Preparation for Litigation

Reporting: Not So fast

What laws govern if there is a data breach?

To whom does the company need to report?

When does the reporting obligation "kick in?" What is an incident? What are the timelines?

New York

New York State Information Security Breach and Notification Act (NY Gen. Bus. Law § 899-aa)

"Breach of the security of the system" means an unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of PI maintained by a business.

The Attorney General can seek injunctive relief and damages for actual costs or losses can be awarded to consumers who were entitled to notice. If there is a finding that the business’s failure to report the data breach was knowing or reckless, then the Court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, not to exceed $250,000.

Business Continuity Plan

COVID-19 forced companies to quickly develop and implement business continuity plans. Did you have one? If not, how fast did you develop it and what does it contain?

- Emergency contact information for internal and external personnel
- Insurance information
- Landlord information; Tenant information
- Team members; Meeting schedules
- Critical Assets: People, Physical Structures, Equipment, Data, Inventory, Operations, Vendors, Customers

Vendor Management Plan

Purpose: to outline the business relationship and expectations between the company and the vendor and to mitigate cyber security risks

Determine how the company and vendor will handle data transfers and data security

Require the vendor to explain how the vendor handles its own data security

Review the vendor’s cyber security policies and insurance

What industry standards apply? What Government standards apply?