Cybersecurity Update—Where Are We Now?

Ashley Madsen, CIPP/US
Data Privacy, Cybersecurity and AI Associate Attorney
Godfrey & Kahn, S.C.
Milwaukee, Wisconsin

Kate H. Campbell, CIPP/E, CIPP/US, CIPM
Senior Counsel
Neal, Gerber & Eisenberg LLP
Chicago, Illinois

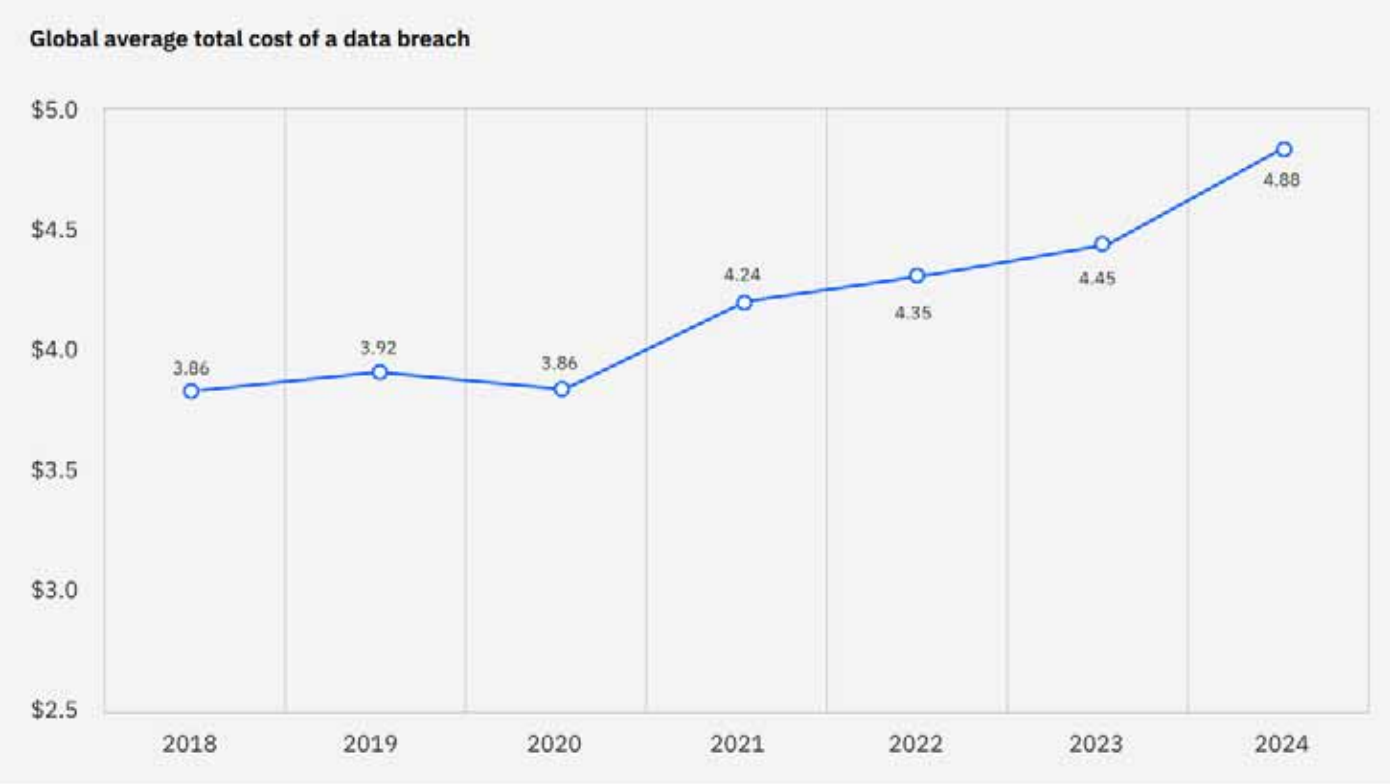
International Foundation of Employee Benefit Plans

Agenda

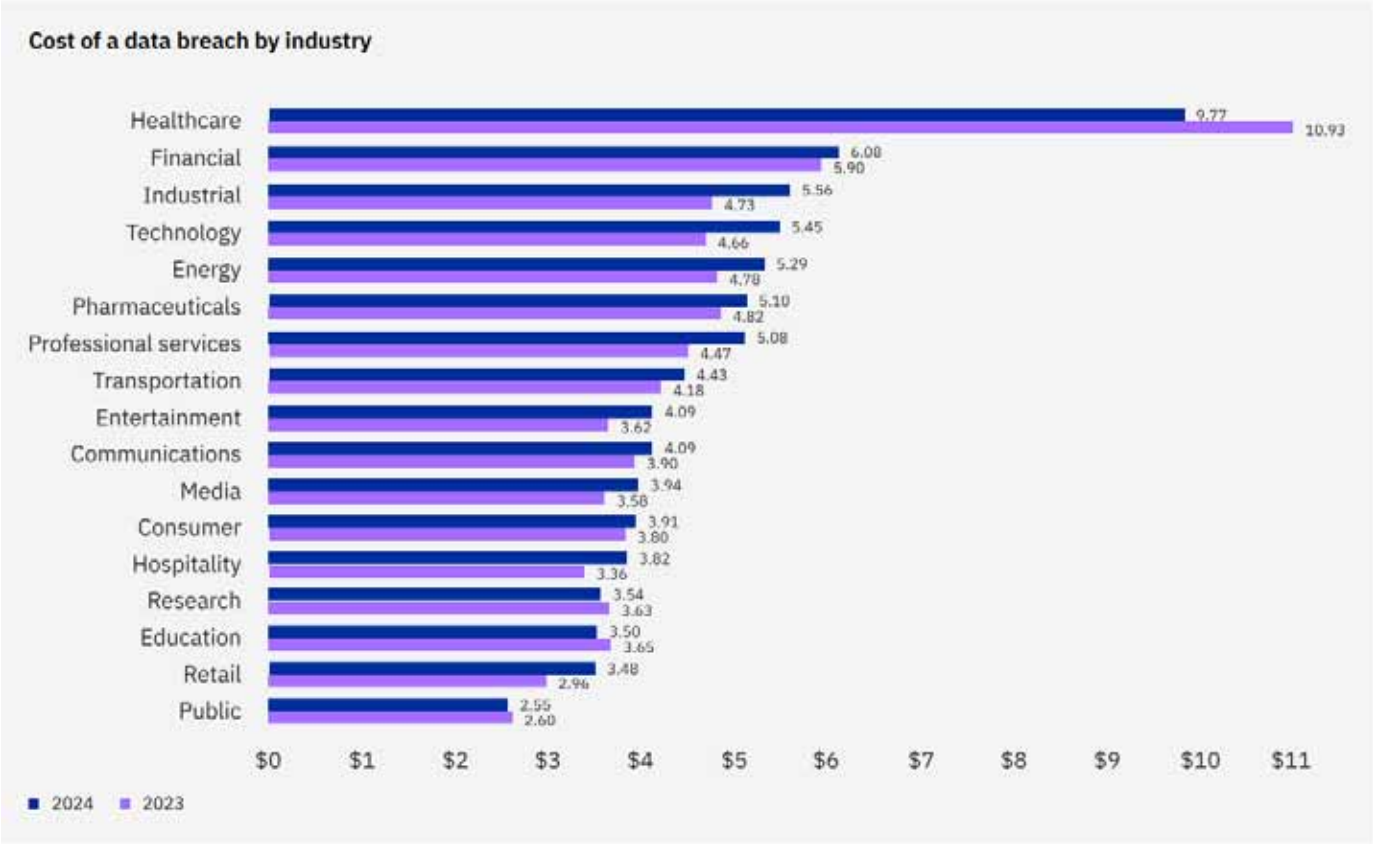
- Costs statistics related to cybersecurity
- Importance of cybersecurity
- Primer on legal obligations
- Best practices for breach response
- Breach response process

PLEASE STOP ME TO ASK QUESTIONS

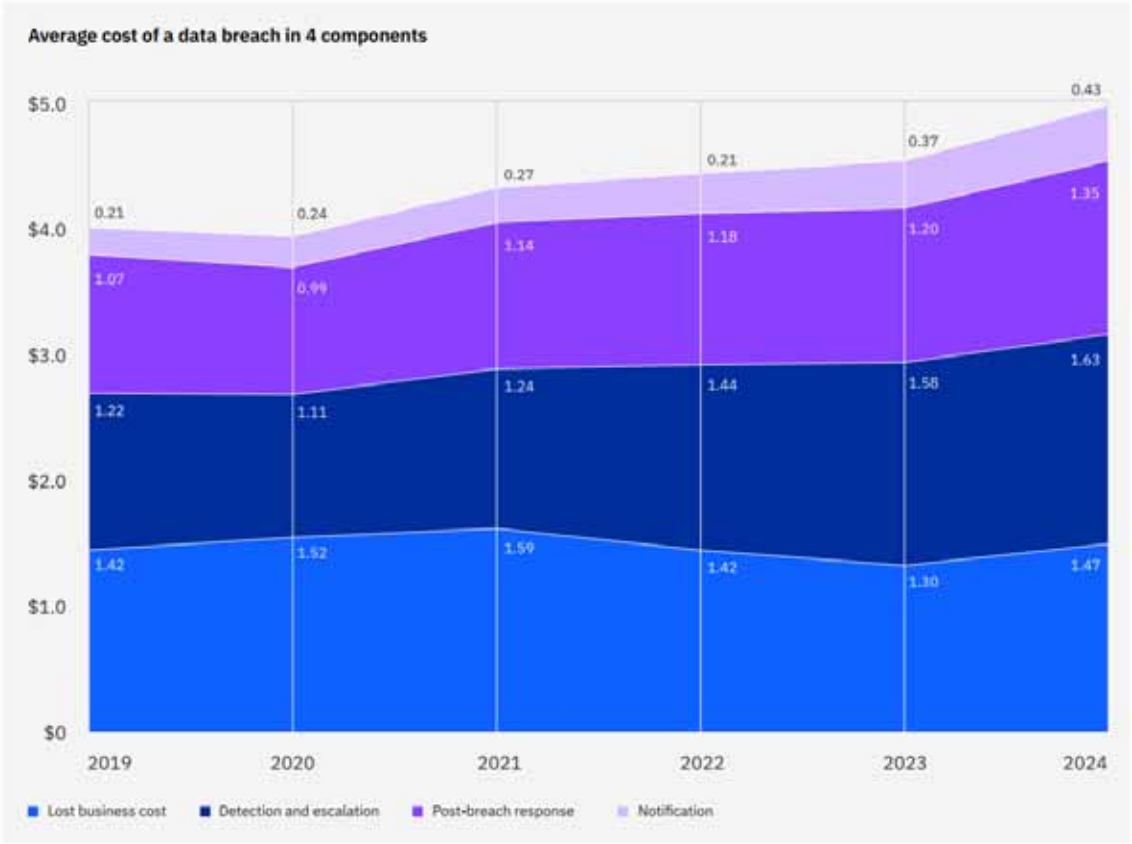
What Are the Costs?



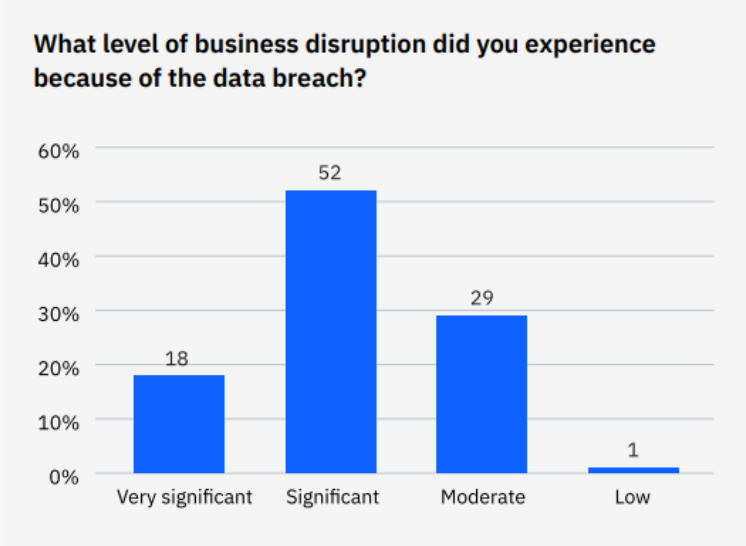
What Are the Costs?

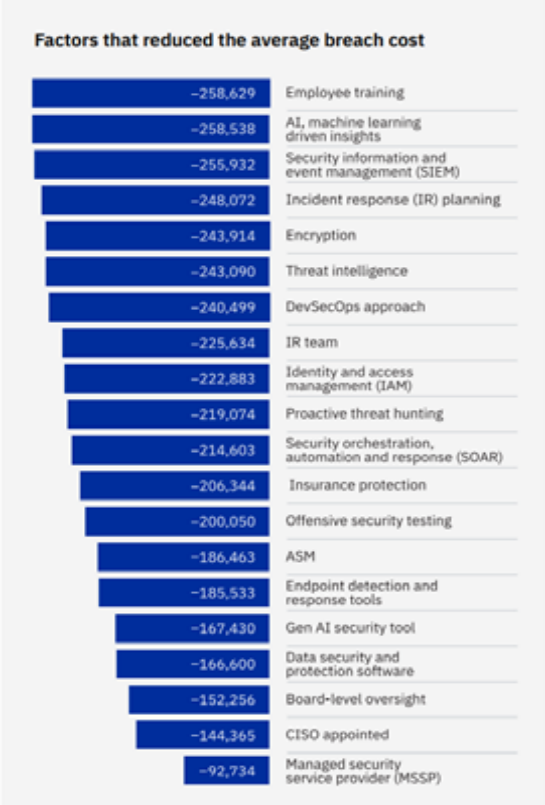


What Are the Costs?



What Are the Costs?





Types of Claims

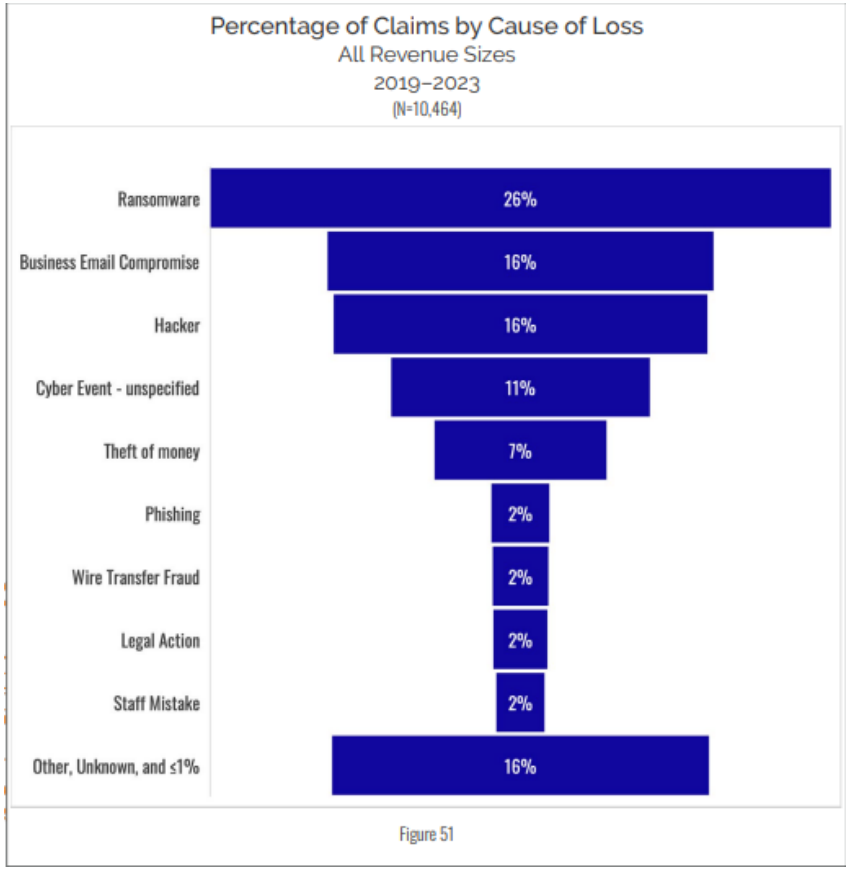
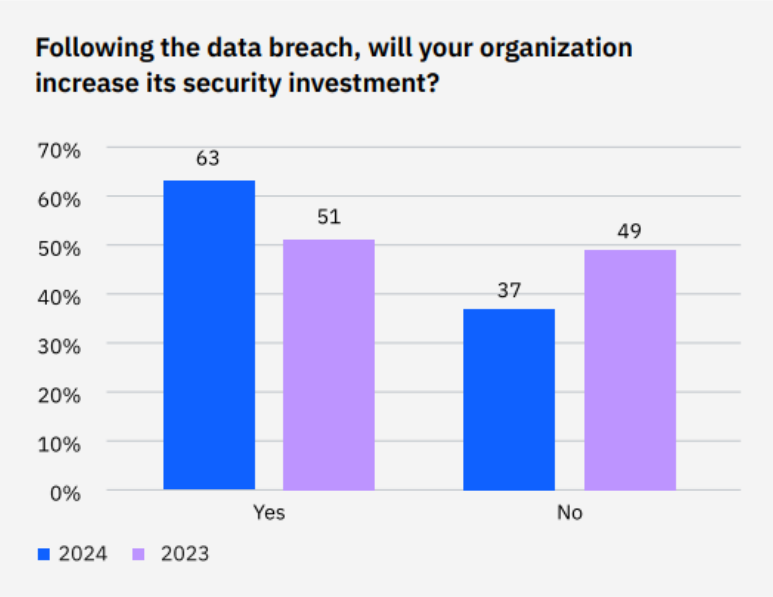
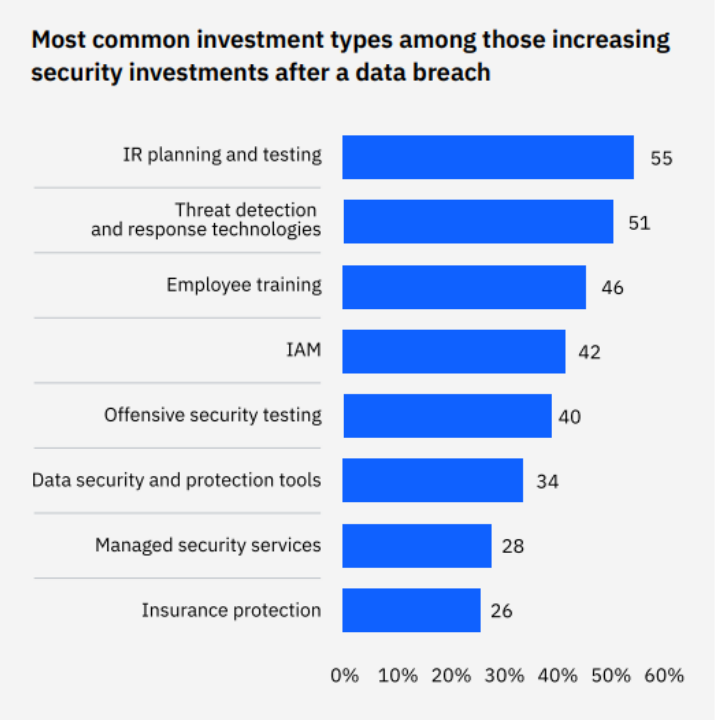


Figure 51

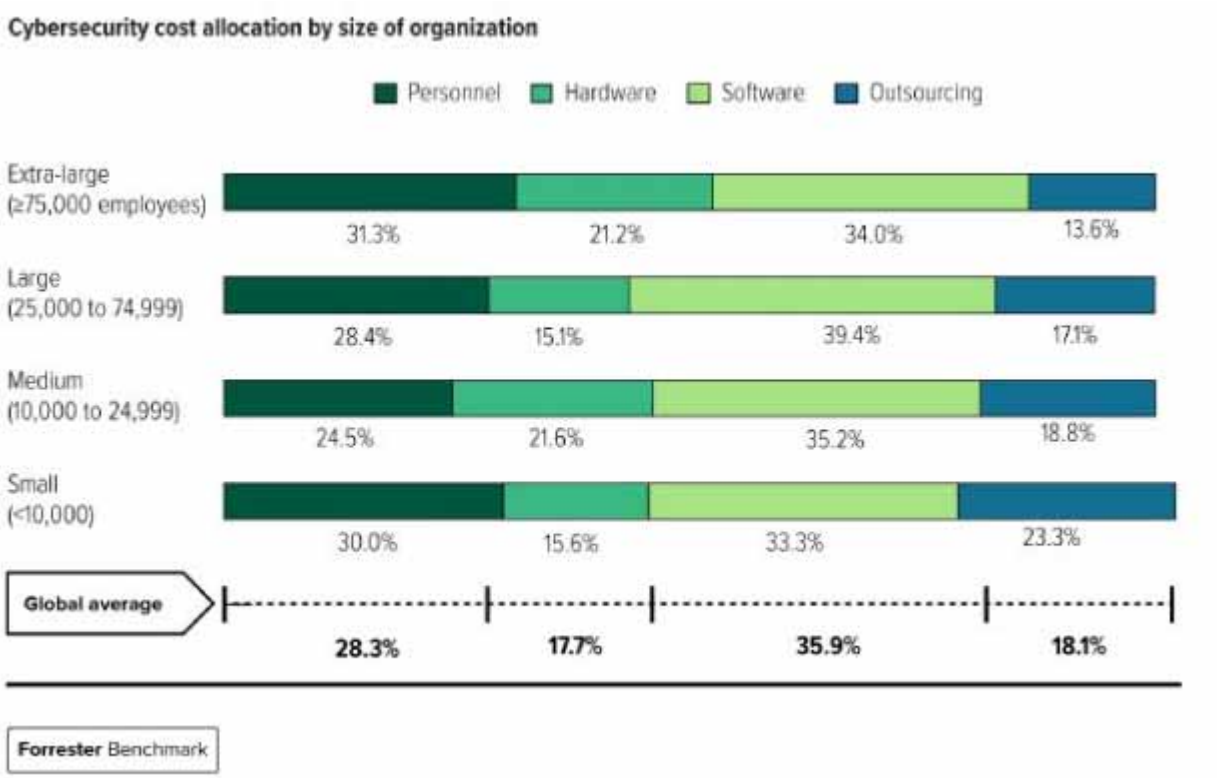
High Costs = High Investment?

Investment

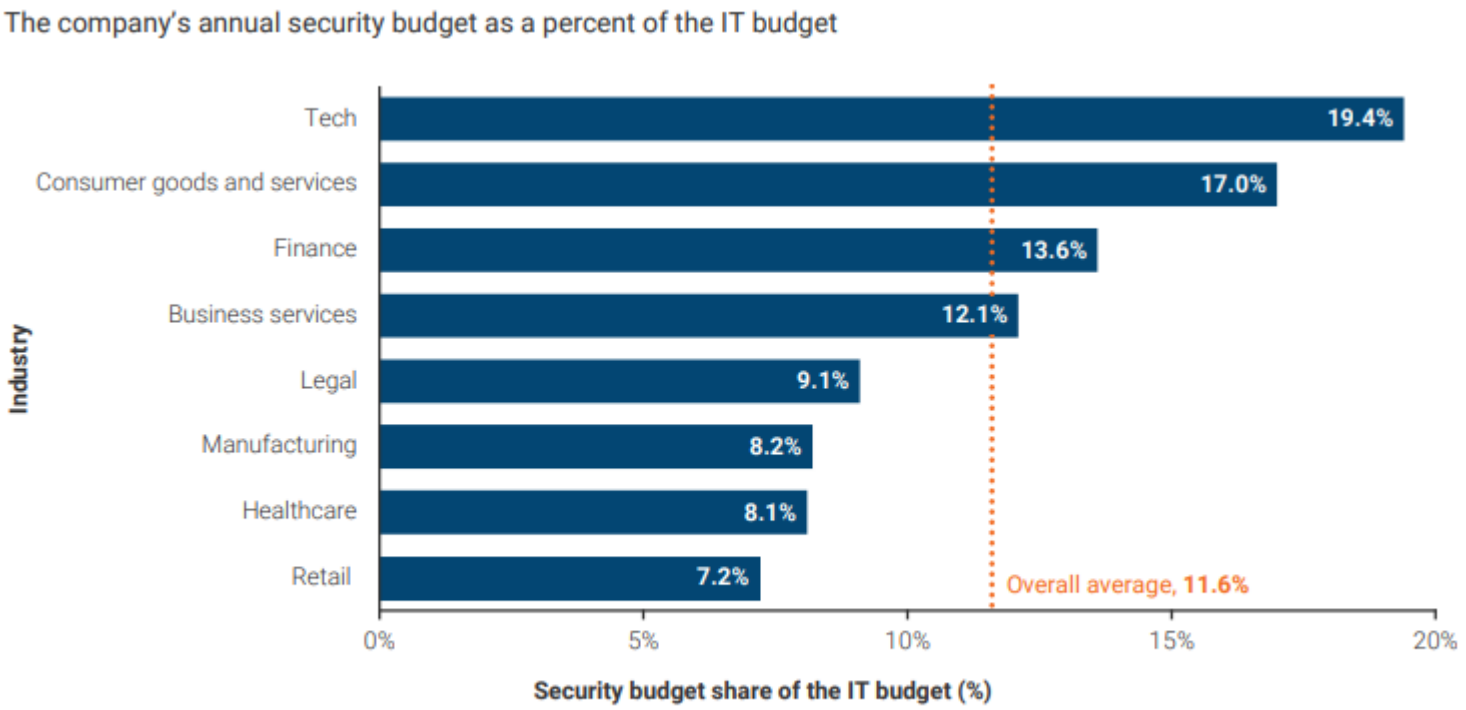

Following the data breach, will your organization increase its security investment?
70%
60%
50%
40%
30%
20%
10%
0%
63
51
37
49
Yes
No
2024
2023


Most common investment types among those increasing security investments after a data breach
IR planning and testing
55
Threat detection and response technologies
51
Employee training
46
IAM
42
Offensive security testing
40
Data security and protection tools
34
Managed security services
28
Insurance protection
26
0%
10%
20%
30%
40%
50%
60%

Organization Size



Investment (Percent of IT Spend)



Setting a Cybersecurity Budget

- Factors that might influence budget
  - Business size
  - Industry
  - Complexity of the business
  - Legal compliance obligations
  - Type of data utilized/processed
    - How sensitive?
  - Cyber insurance requirements

Setting a Cybersecurity Budget

- Making a budget
  - Evaluation of existing cybersecurity posture
  - Identification of key assets
  - Prioritize the allocation of budgets
  - Consider both short-term and long-term requirements
  - Allocate funds to expedite incident response and recovery
  - Review and update the budget regularly
  - **Management buy-in**

Importance of Cybersecurity: Why Should It Matter to You?

Concerns

- Benefit plans are a prime target
- Health care sector most targeted
- Retirement plans also under fire
- 86% of breaches were financially motivated and 10% were motivated by espionage
- High costs associated with data breaches
- Reputational concerns
- Legal obligation

Common Threats

Our Plans Are Being Targeted

- Why are benefit plans a popular target?
  - Plans host a lot of sensitive information
  - Access to large sums of money
  - Plans use a variety of third-party service providers, consultants, agents, etc., each of which is susceptible to supply chain attacks
  - Cybersecurity often not been treated as a priority
- Trends
  - Recent uptick in ERISA fiduciary litigation involving TPAs and plans, and ransomware events involving deep dives into an entity's finances and high ransoms

Risk to Assets

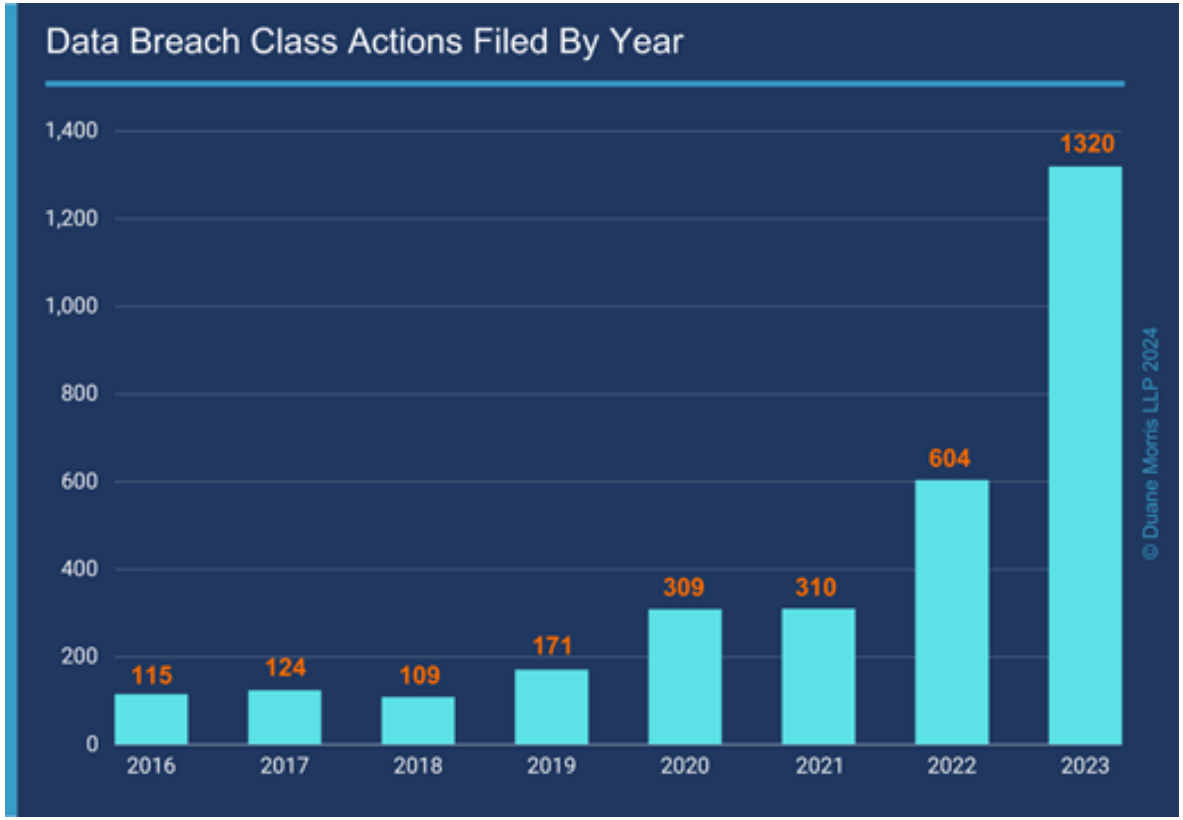
- Insufficient cybersecurity controls in retirement and health plans risks the personal assets and property of:
  - Board members
  - CEO, CFO, Chief HR Officer
  - Committee members
  - Any employees with some measure of authority over the plan.

Legal Obligation

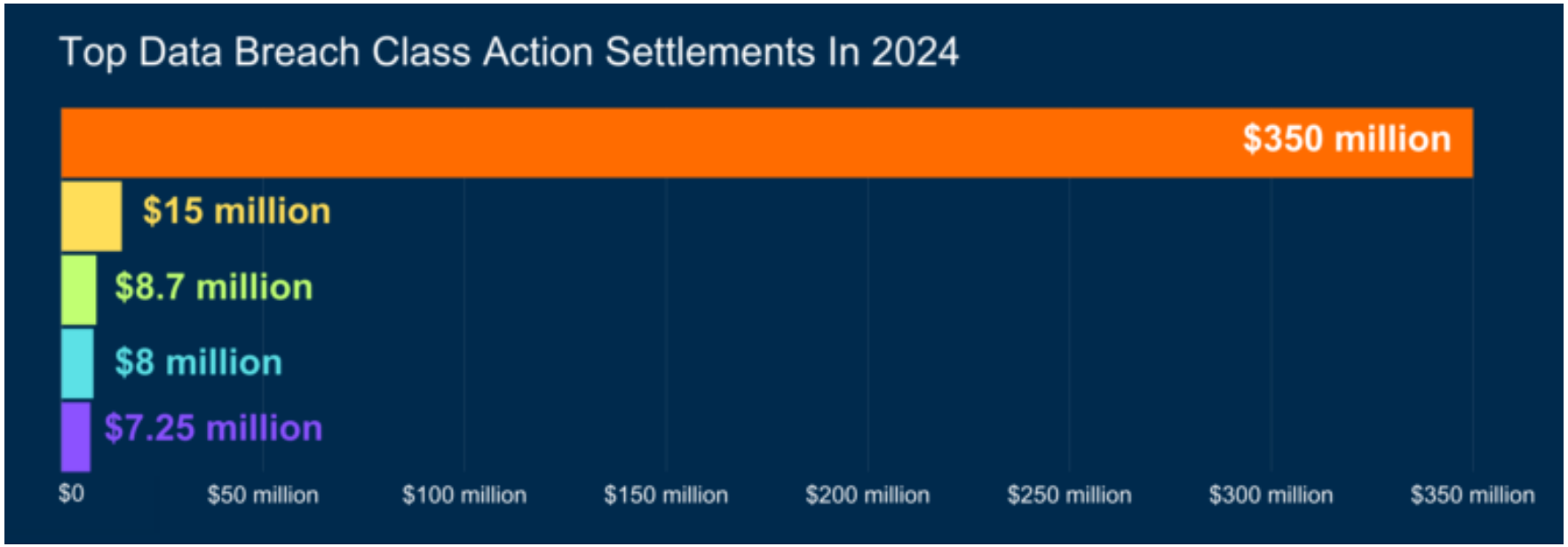
- ERISA: Fiduciary Duty
- HIPAA: Security Rule and Privacy Rule
- State Statutes
  - Comprehensive Privacy
  - Breach Notification
- Common Law
  - Trust: “Reasonable steps” to control/protect
  - Negligence: Duty of “reasonable care”

IT’S THE LAW

Potential Litigation



Biggest Settlements of 2024



A Primer on Legal Obligations

Legal Obligations Involving Security

- Legal obligations of trustees and administrators
  - Under ERISA, those with authority or control over plan management or administration have a fiduciary duty to participants and beneficiaries

Trustee Legal Obligations

- Duty of Loyalty
- Prudent Administration of Trust
- Duty to exercise reasonable care, skill, and caution
- Control and Protection of Trust Property
- “A trustee shall take reasonable steps to take control of and protect the trust property.” *See* Restatement (Second) of Trusts §§ 170, 174, 176.

Fiduciary Obligations

- Fiduciaries must exercise a “Duty of Prudence” when working with service providers
  - Carefully select plan service providers
  - Ensure appropriate cybersecurity controls are in place
  - Review contracts to confirm that rights and responsibilities for incidents and data handling are appropriately distributed
  - Regularly monitor and/or audit to confirm compliance

Standard of Care

- All plans must (at a minimum):
  - Ensure confidentiality and integrity of data
  - Protect against reasonably anticipated threats
  - Protect against unauthorized use or disclosure
  - Ensure compliance by employees
  - Actively detect and remediate problems.

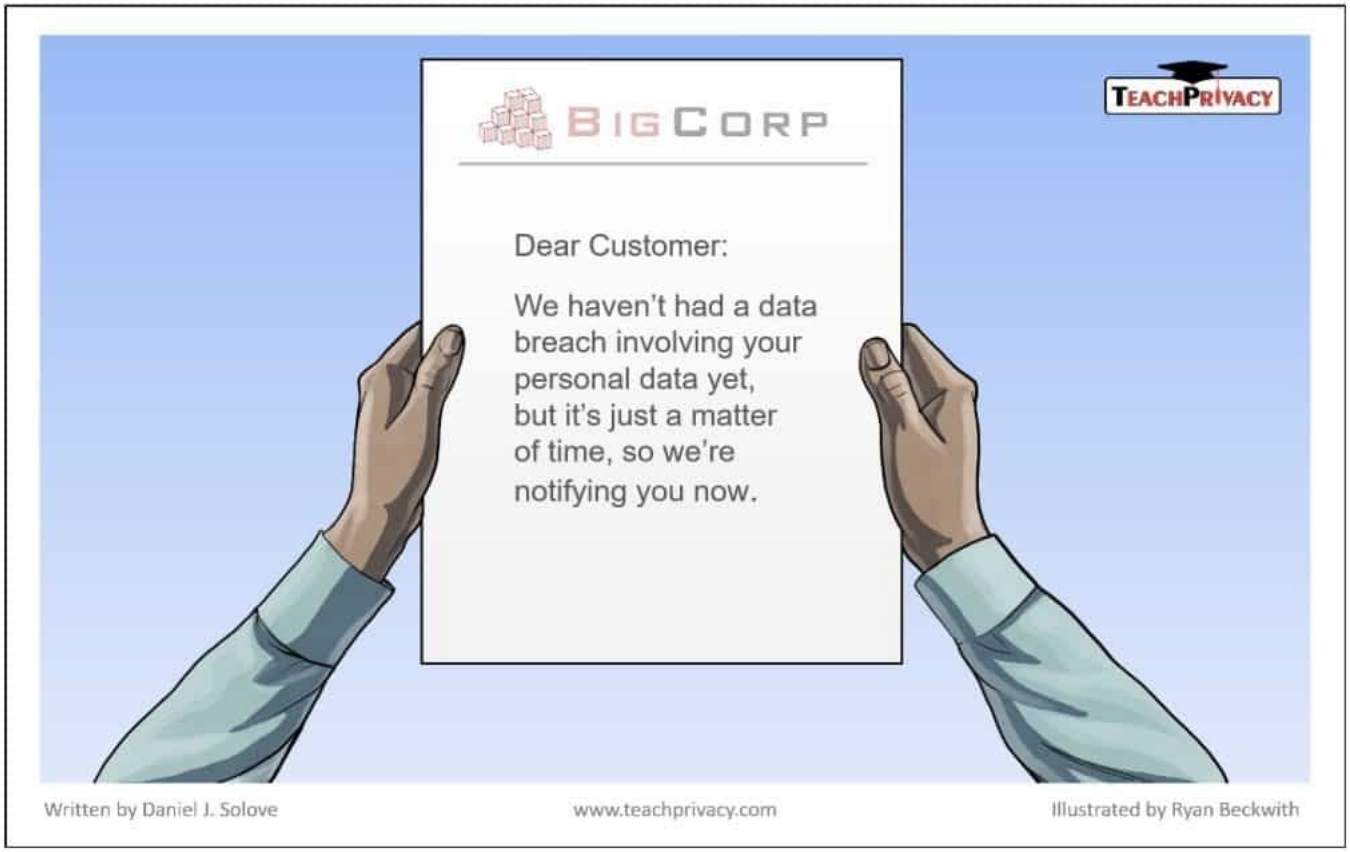
Department of Labor Guidance

- December 2024 Guidance from DOL addresses Cybersecurity
  - Compliance Assistance Release No. 2024-01
    - Tips for Hiring a Service Provider
      - Prudent selection of service providers and active monitoring
      - Insurance verification
      - Contractual terms relating to cybersecurity
      - Compliance with applicable privacy and security laws
    - Cybersecurity Best Practices
      - Responsibilities to manage risks
      - Hiring service providers that follow best practices
      - Sensitive Data encryption
      - Security training
    - Online Security Tips (for participants/beneficiaries)

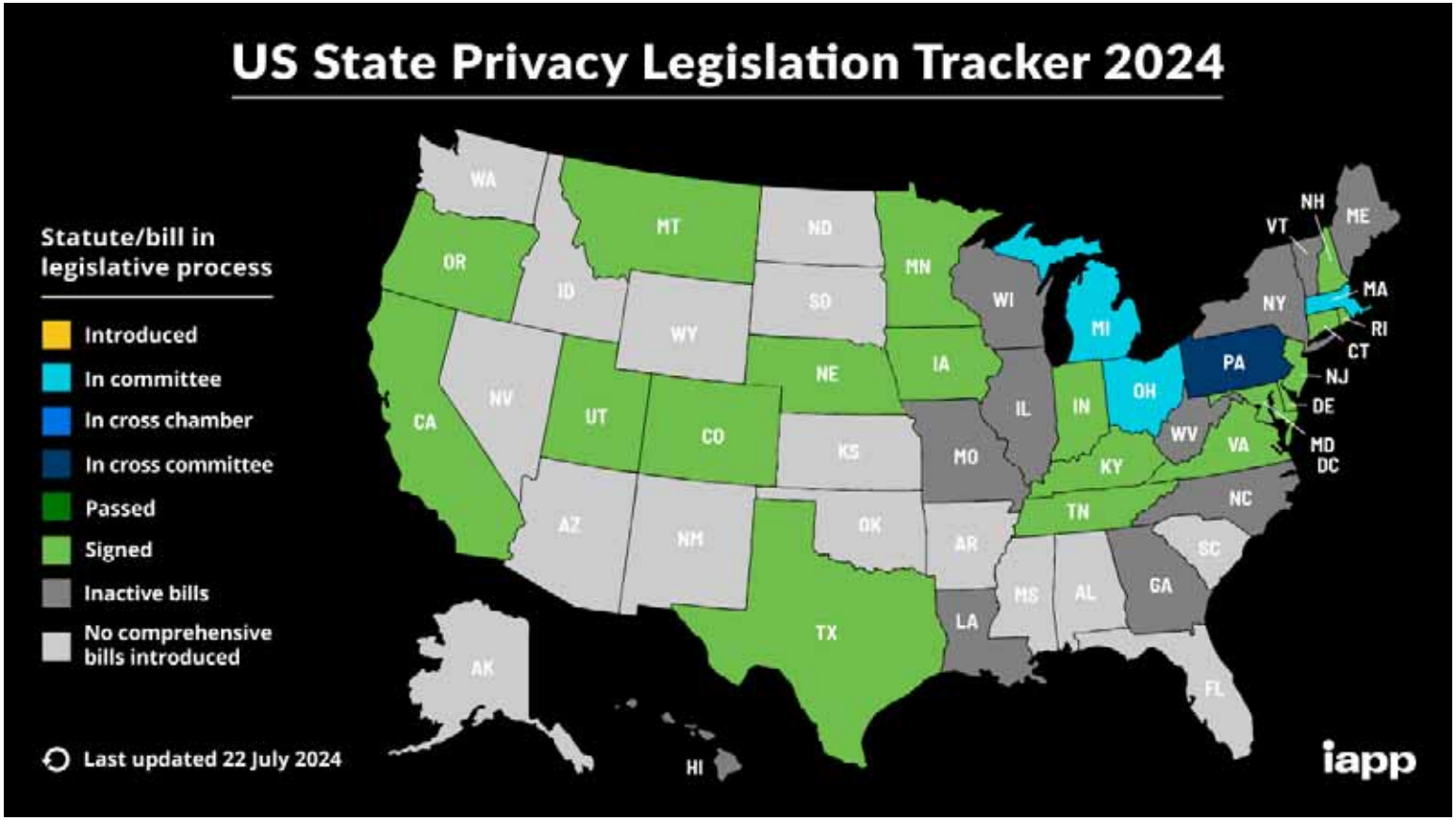
HIPAA Security Rule

- Applies to covered entities (plans) and business associates
- Has the business associate…
  - Done a risk analysis?
  - Implemented security measures?
- Settlements with HHS for data breaches since 2020
  - University: $875,000 for 280,000 people ($3.13/person)
  - Insurer: $5.1M for 9.3M people ($0.54/person)
  - Insurer: $6.85M for 10.4M people ($0.66/person)

State Data Breach Laws



State Privacy Laws



Common Law

- Trust
  - "Reasonable steps" to control and protect...
    - *See* Restatement (Second) of Trusts §§ 170, 174, 176.
- Negligence
  - Duty of "Reasonable Care"
    - Reasonableness of cybersecurity measures

Best Practices

Reasonable Security Measures

- What does “reasonable security measures” mean for companies, regardless of industry?
  - Having policies and procedures in place
  - Having an Incident Response Plan
  - Utilizing security best practices
    - Strong passwords
    - Vulnerability/penetration testing
    - Intrusion detection system
    - Encryption

Read and Follow This

U.S. DEPARTMENT OF LABOR

US DEPARTMENT OF LABOR UPDATES CYBERSECURITY GUIDANCE FOR PLAN SPONSORS, FIDUCIARIES, RECORDKEEPERS, PLAN PARTICIPANTS TO PROTECT INFO, ASSETS

https://www.dol.gov/newsroom/releases/ebsa

https://www.dol.gov/newsroom/releases/ebsa/ebsa20240906-0

Read and Follow This

U.S. DEPARTMENT OF LABOR

12 Cybersecurity Program Best Practices

1. Have a Program
2. Risk Assessments
3. 3rd Party Audits
4. IS Roles and Responsibilities
5. Access Control Procedures
6. Cloud Storage Security Reviews
7. Cybersecurity Training
8. Secure SDLC Program
9. Business Resiliency Program
10. Encryption
11. Technical Controls
12. Incident/Breach Response

Our Recommendations

- Have a Written Information Security Policy
  - Asked for by State AGs and federal regulators as a matter of course
  - Part of the DOL Guidance

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate.**
- **Restore normal operations and services.**

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

Our Recommendations

- Have an Incident Response Plan
  - Pre-identify a “breach coach”—A cybersecurity attorney to assist you
  - Pre-identify forensics provider
  - Use $0 retainers
  - Get breach coach and forensics provider approved by your insurer before an incident

Our Recommendations

- If you don't practice your Incident Response Plan, burn it
  - Need to conduct routine table-top exercises
  - Build muscle memory
  - Know who to call
  - What if comms are down?
  - Who decides to pay a ransom?

Our Recommendations

- Employee trainings
  - Phish your own employees
  - Conduct annual cybersecurity training
  - Don’t just focus on email—Talk about other methodologies
  - Train customers to recognize persuasion
  - Hire penetration service testers to test your systems and employees

Our Recommendations

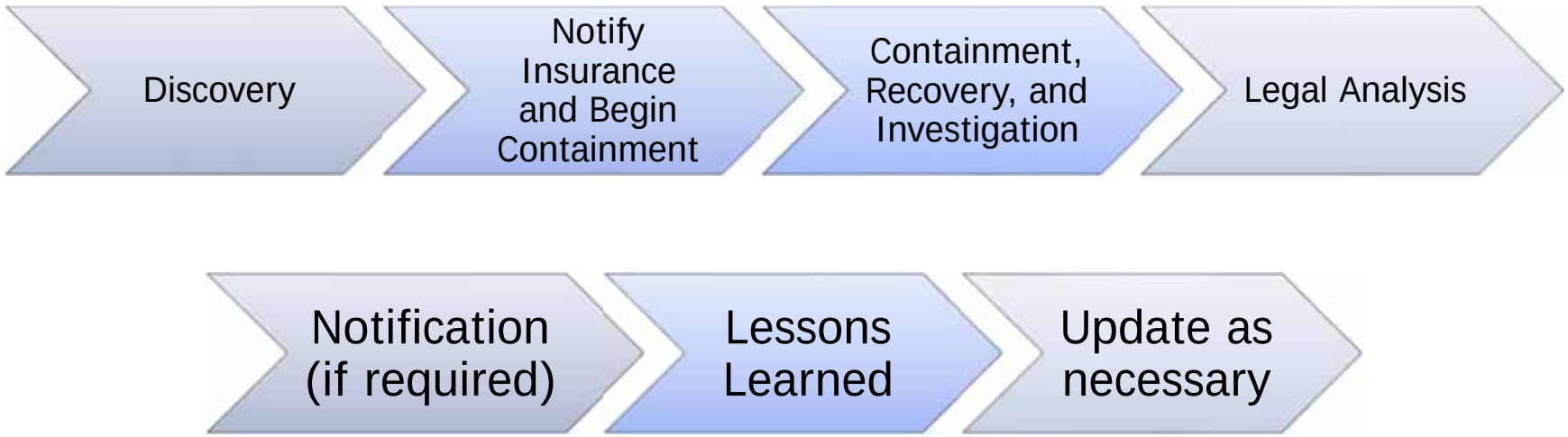
- Layered security
  - Annual/bi-annual employee training
  - Internal policies
  - Strong password requirements
  - Vulnerability scans
  - Phishing tests
  - Penetration tests
  - Outgoing payment controls
    - Segregation of duties and dual authorization
    - Confirmation of any changes to vendor details

Our Recommendations

Address vendor risk

Breach Response Basics

Breach Response Process



Initial Steps

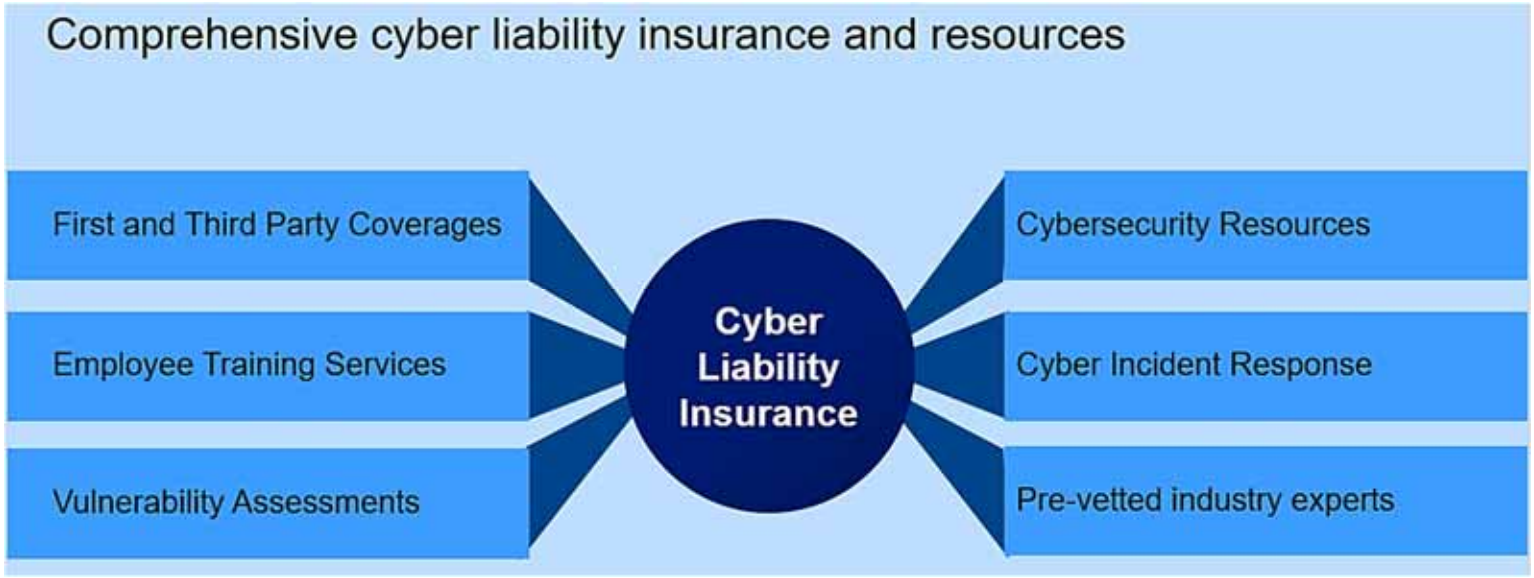
- Ideally, company already has an Incident Response Plan
  - Follow the plan
  - Call the team together
  - Work down the call chain
    - Attorney
    - Insurance company
    - Bank (if applicable)
    - Law enforcement (business decision)

Initial Steps

- Preserve records
- Pull insurance policies, relevant contracts, bank information (if wire fraud)
- Control communications internally and externally
- Utilize attorney-client privilege
- Initiate and cooperate with forensic investigation
- Notify your cyber carrier

Cyber Liability Insurance

- What does cyber liability coverage offer?



How Are Cyber Claims Handled?

- Step 1: You report breach to carrier
- Step 2: Carrier refers to breach counsel (may have a reservation of rights)
- Step 3: Breach counsel engages incident response team (forensics, crisis PR, etc.)
- Step 4: Invoices for the above service are submitted directly to carrier for payment

“Watch and Wait” Approach

- Exception to the “Watch and Wait” approach: Ransomware
  - If you receive ransom note, or have a reasonable belief there is ransomware, taking the server or computer offline can prevent the entire machine from being encrypted
  - Flip side: You can also lose files due to a broken encryption process

Investigation

- Goal is to determine the scope of the incident and collect evidence
- In most scenarios, organizations use a third-party forensic provider
- You should also use outside breach counsel
- Think carefully about what documentation of the security incident is created

How Can Experts Assist During a Breach?

- Determine the scope
- Secure the systems
- Work closely with counsel to determine what data, if any, was compromised
- Provide cybersecurity recommendations moving forward
- Serve as an ongoing resource

Remediation

- Recover systems and data to the extent possible
- Determine notification obligations under state, federal, international law, and client agreements
- Analyze contractual obligations and make required notifications

Organization Name	Date(s) of Breach	Reported Date
Landry's, Inc.	01/18/2019, 10/17/2019	12/31/2019
Legalinc Corporate Services, Inc. (as data maintainer) on behalf of Stripe GEP, Inc. (as data owner)	10/25/2017, 12/04/2019	12/31/2019
Evolucion Innovations Inc.	11/08/2019	12/31/2019
Active Network, LLC	10/01/2019, 11/13/2019	12/30/2019
SharesPost, Inc.	09/06/2019	12/27/2019
ACCO Engineered Systems, Inc.	11/20/2019	12/26/2019
Avid Technology, Inc.	10/08/2018, 10/12/2018	12/24/2019
HelloTech, Inc.	n/a	12/23/2019
Moss Adams LLP	10/08/2019, 10/10/2019	12/22/2019
Jambav, Inc.	n/a	12/19/2019
Island Restaurants, LP and Champagne French Bakery Cafe	02/18/2019, 09/27/2019	12/19/2019
Wawa, Inc.	03/04/2019, 12/12/2019	12/19/2019
Western Health Advantage	10/20/2019	12/13/2019

Data Breach Notification

- Victims—Laws vary state to state, and internationally, as does legal liability
- May require notice to the state attorney general, foreign governmental agency, and/or data protection authority, sometimes depending on number of records compromised
- Laws have varying times for notification

Wrap-Up

- Team meeting to discuss lessons learned
- Review policies and adjust accordingly
- Create action list for security improvements

Key Takeaways

- Make knowledgeable and effective cybersecurity budgeting decisions
- Stay up to date on risks and legal requirements
- Prepare for the worst
- Scrutinize your vendors
- Practice your plan
- Train and educate your employees

Your Feedback Is Important. Please Scan This QR Code.

Session Evaluation

Questions?


NEXT TIME
YOU'LL TAKE SECURITY AWARENESS TRAINING SERIOUSLY