



Cybersecurity Conference

Wednesday, January 24, 2024

The US Privacy and Security Landscape



January 24, 2024
Michelle L. Merola
Gary M. Schober

US Privacy/Security Landscape

- In California, for example, personal information is **information** “that identifies, **relates to**, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with **a particular consumer** or household.” Other jurisdictions have similar definitions.



- Privacy laws are designed to provide individuals with certain rights over their personal information.

Disclosure

Control

Security



What Inspired US Privacy/ Security Law?

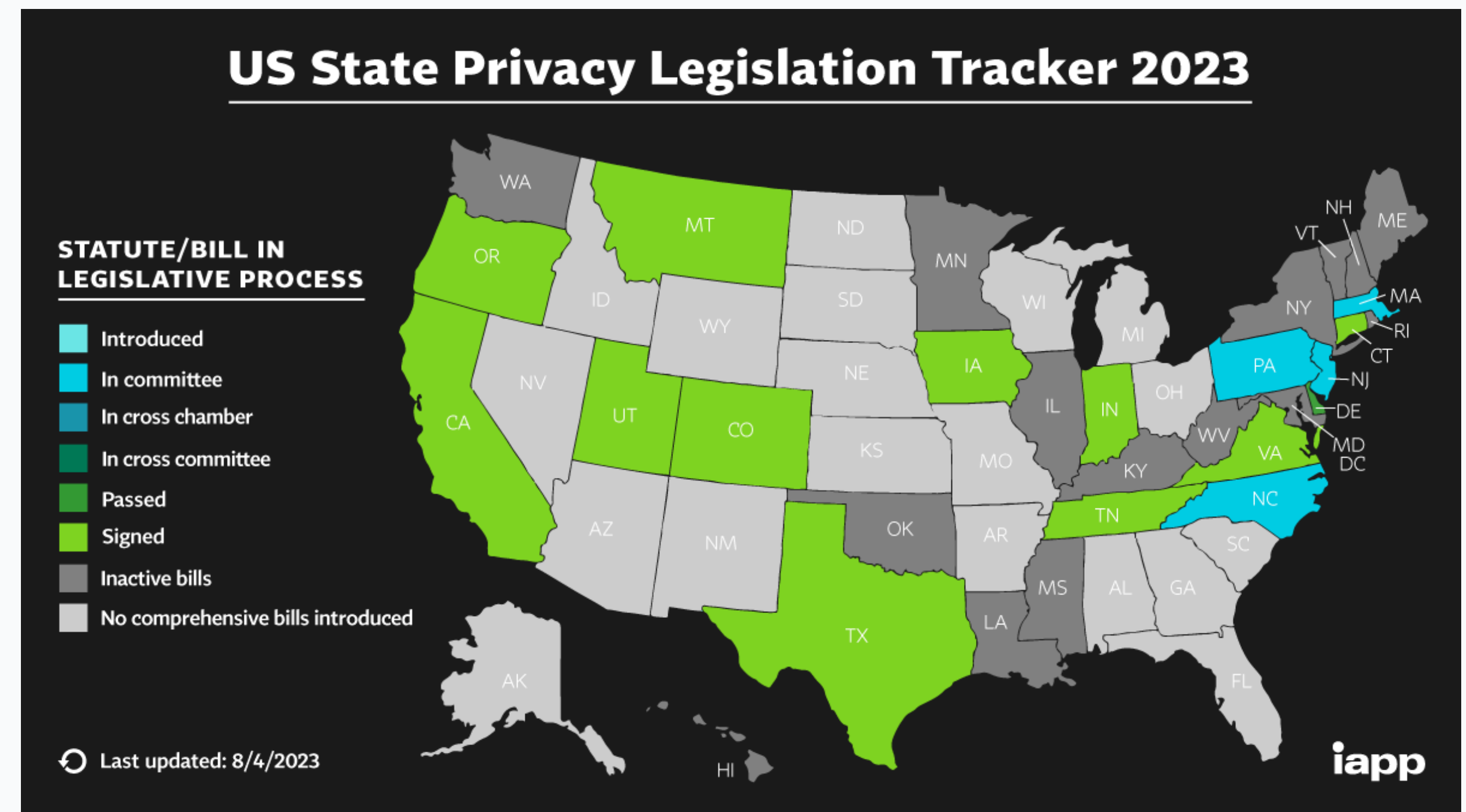
General Data Protection Regulation (EU GDPR)

- Replaced the E.U. Privacy Directive on May 24, 2018.
- Requires transparency so that data subjects know what data is being collected and how it is used.
- Provides data subjects with access to their personal data and the right to have data corrected or deleted.
- Processing must be for a legal purpose.
- Only data necessary for a legal purpose can be processed or retained (i.e. minimization requirement).
- “Adequacy” needs to be established for international transfers of data. The E.U.-U.S. Privacy Shield was recently invalidated by the E.U. Standard contractual clauses and binding corporate rules can be used.

Emergence of State *Privacy* Laws

As of today, thirteen US states have enacted comprehensive data privacy laws:

- California (1/23)
- Colorado (7/23)
- Connecticut (7/23)
- Delaware (1/25)
- Indiana (1/26)
- Iowa (1/25)
- Montana (10/24)
- Oregon (7/24)
- Tennessee (7/25)
- Texas (7/24)
- Utah (12/31/23)
- Virginia (1/23)
- New Jersey (1/25)



But many more to come . . .

including New York

(All states have breach notification laws.)

What Are the General Obligations of Businesses Under US Privacy Laws?



▪ Notice/disclosure



▪ Recordkeeping



▪ Consumer requests



▪ Equal treatment




▪ Security



▪ Training



▪ Opt out/in of sales



What is the California Consumer Privacy Act (CCPA)?

- CCPA is a consumer rights statute.
- Applies to for-profit businesses that do business in California and meet any of the following criteria:
 - Gross annual revenues over \$25 million.
 - Buy, sell, or share the personal information of 100,000 or more consumers or households.
 - Derive 50% or more of their annual revenue from selling or sharing consumers' personal information.
- Doing business in California could be broadly defined.
- Privacy policies must contain California-specific provisions.



Is the California Privacy Rights Act (CPRA) Something Different?

- Amends the CCPA and went into effect January 1, 2023.
- Enhances the rights of consumers and obligations of businesses.
- Establishes a new sub-category of personal information called “sensitive personal information.”
 - SSN, state identification card, precise geolocation information, racial or ethnic origin, and biometric identification, among other things.
 - Businesses collecting sensitive personal information are required to notify consumers at or before the time of collection of (1) the category of information collected; (2) the retention period; and (3) whether such information is sold by the business.
- Extends its reach to employees’ personal information and personal information shared among businesses.



Polling Question #1

- The California Consumer Privacy Act applies only to businesses in the State of California.
 - **TRUE**
 - **FALSE**



Core Privacy Issues: Consent

What is consent?

Any freely given, specific, informed and unambiguous indication of an individual's agreement to the processing of personal data relating to him or her.

Types:

- Opt-in and Opt-out: Opt-in systems require consent prior to processing personal data.
- Affirmative/Explicit Consent: An individual "signifies" his or her agreement by some active communication between the parties.
- Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual, ex., consent inferred from use of website.



Generally, How Do You Get Consent?

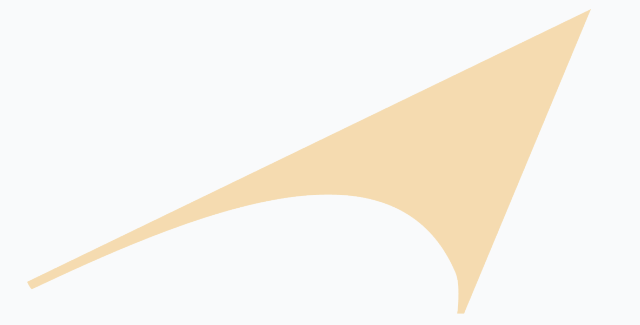
General Rule

- If you provide notice of your data handling practices (with a link to your privacy policy) at the time of collecting the data and provide the opportunity to opt-out of the collection, you can collect and use the data right away without any confirmation from the person.

Exceptions

- Most laws require the prior consent to sell the personal information for children (definitions range between 13 and 16).

Core Privacy Issues: Sale of Data and “Sharing” Data



California Do Not Sell or Share

Use Transcend to comply with California's "Do Not Sell or Share My Personal Data" opt-out requirements under CCPA and CPRA, including requests received via browser privacy signals like [Global Privacy Control](#). Completing this guide will also help ensure compliance with requirements of state privacy laws in Virginia, Colorado, and Utah.

While we do our best to provide general background about regulatory issues, this guide is provided for informational purposes only, and should not be construed as legal advice. You should consult with your legal counsel on any specific CCPA questions you have.

Quick Facts

- The **California Consumer Privacy Act (CCPA)** is in effect and gives California residents the right to opt out of the sale of their personal information, with the opt-out offered via a prominent "Do Not Sell My Personal Information" link on the "selling" party's homepage.



Do Not Sell My Personal Information

Do Not Sell My Info



What is Selling, Sharing, and Disclosing?

- “Selling” is “communicating ... personal information ... to a third party for monetary or other valuable consideration.”
- “Sharing” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information to a third party for *cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.
 - *Cross-context behavioral advertising is defined as the targeting of advertising to a consumer based on consumer’s activities across businesses.*
- “Disclosing” is undefined but is everything else. For example, providing access to vendors that assist with operations.



How Do Businesses Comply With the Do Not Share or Sell Requirements?

- Businesses that sell personal information may be subject to the requirement under certain state privacy laws to provide a clear and conspicuous “Do Not Sell My Personal Information” link on their website that allows you to submit a request to opt-out of the sale of personal information to ***third parties***. Businesses cannot require you to create an account in order to submit your request.
- Under certain state privacy laws, businesses that do targeted advertising may be required to provide a clear and conspicuous “Do Not Sell or Share My Personal Information.”



Polling Question #2

- Some state privacy laws require businesses to provide a clear mechanism to consumers for opting out of targeted advertising.
 - **TRUE**
 - **FALSE**

Who is the Privacy/Security Cop?

National Level

The FTC has been the primary federal agency on privacy policy and enforcement, filling a regulatory void. Rapid changes in technology and E.U. pressure have increased privacy challenges. The FTC continues to rely on Section 5 of the FTC Act, which prohibits “unfair and deceptive trade practices.”

- FTC has been expanding its jurisdiction.
- Increased technical safeguards required in FTC settlements (ex. Café Press).

State Level

- State Attorneys General.
- Special agencies like the California Privacy Protection Agency (CPPA).



Do Any of These State Privacy Laws Incorporate Data Security Requirements?

- Some require businesses to “implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.”
- Some also require businesses to conduct annual cybersecurity audits and prepare risk assessments.
- The CPRA creates a private right of action for data breaches that result from inadequate security.
(pending New York legislation may do the same).



Security Concerns

Surreptitious Acquisition of Data (bad actors)

- Phishing Attacks
- Ransomware
- Business Email Compromise (BEC)
- Spoofing
- Watering Hole Attacks
- Pharming
- Exploiting Cloud Vulnerabilities

Inadvertent Disclosures of Regulated Data

Examples

- Disclosures Without Proper Consent
- Web Tracking Technologies
 - State AG Offices
 - FTC Enforcement Actions
 - Class Actions



Polling Question #3

- Security of personal information is typically not addressed in the emerging state privacy laws.
 - **TRUE**
 - **FALSE**



Do Vendor Contracts Need to Address Privacy and Cybersecurity Under These Laws?

- **Yes, and they should:**
 - Limit the use of personal information to the specified contractual purpose.
 - Obligate the vendor to comply with applicable privacy obligations.
 - Give the business the right to take reasonable and appropriate steps to ensure that the vendor uses the personal information in a manner consistent with the business's legal requirements/obligations.
 - Require the vendor to notify the business if it determines it can no longer meet its obligations under the CPRA.
 - Give the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

Contractual Requirements (Cont.)

- The contract must state that the service provider or contractor is prohibited from:
 - Selling or sharing personal information.
 - Retaining, using or disclosing personal information for any purpose other than for the business purposes specified in the contract.
 - Retaining, using or disclosing the information outside of the direct business relationship between the service provider/contractor and the business.
 - Combining the personal information it receives under the contract with personal information it receives itself or from other entities.
- The vendor must pass the requirements down to sub-contractors through a written agreement.
- The vendor should certify that it understands the restrictions on it and will comply with them.

Questions?



HODGSON RUSS
Contact Us



MICHELLE MEROLA

Partner

mmerola@hodgsonruss.com

518.736.2917



GARY M. SCHOBER

Partner

gschober@hodgsonruss.com

716.848.1289



A Lawyer's Guide to Cyber Insurance



January 24, 2024
Ryan K. Cummings



Insurance Primer

- Coverage Types
 - First Party
 - Third Party
- Policy Period Coverage Type
 - Occurrence
 - Claims-Made
- Policy Components
 - Agreement
 - Exclusions
 - Conditions
 - Endorsements



The Cyber Risk and Its Costs

- Data Breach
 - Theft of customer data or proprietary and confidential business information for purposes of extortion or resale.
 - Consequences can include civil litigation (*e.g.*, consumer class actions); mandatory provision of credit monitoring for affected customers; regulatory and law enforcement investigations, proceedings, fines, and penalties; necessary technical costs to remediate network.
- Ransomware Attack
 - Strong arm takeover of network.
 - Resolution may require ransom payment, breach counsel, forensic investigation, PR consultation, technical remediation.
 - Losses can include lost revenue.
- E-Crime
 - Fraudulent payment instructions; funds transfer fraud.



Polling Question #1


What is "Silent" Cyber Insurance?

- A. Specialized insurance for cyber exposure that can be added on to other policies.
- B. Cyber Insurance for claims against the insured.
- C. Insurance for cyber risks available in legacy insurance coverages.
- D. None of the above.



Answer to Polling Question #1

C. Insurance for cyber risks available in legacy insurance coverages.



“Silent” v. Affirmative Cyber Insurance Coverage

- Insurance for Certain Cyber Exposures May Exist in Standard, Legacy Coverage.
- Commercial General Liability Insurance.
 - Property damage coverage found to apply to Target Corporation’s costs for replacement of affected customers’ credit cards as a result of 2013 data breach. *See Target v. ACE American Ins. Co.*, 19-cv-2916 (D. Minn. Mar. 22, 2022).
 - Personal and advertising injury coverage found to apply to Landry’s costs to defend suit by credit card payment processor for costs arising from data beach affecting customers. *Landry’s, Inc. v. Ins. Co. of the State of Pennsylvania*, 4 F.4th 366 (5th Cir. 2021).
 - Errors and Omissions Liability Insurance, Directors and Officers Insurance, and Standard Property Insurance Could All Provide Some Coverage.
- Cyber Exclusions.



The Cyber Insurance Marketplace

- Comparatively Immature Product-Wise
 - No “standard” coverage.
 - Evolving threat space.
- Difficult Risk Environment Has Raised Premiums
 - Increase in cyber events; increase in size of ransomware demands.
 - Comparatively small risk pool and dependence on reinsurance.
 - Substantial self-insured retentions.
- Specialized Underwriting Process
 - Carriers often require preexisting IT risk management procedures before considering taking on the risk (*e.g.*, multi-factor authentication, password policies, offsite network backup, contracted network security providers, etc.).



Available Coverages

- No “standard” insuring agreement, but categories of first and third-party coverages are available.
- Policies are often à la carte, with various sub-limits of liability for each selected coverage.
- Typically, “claims-made” policies.
- Little litigation over coverage to date.



Polling Question #2

What is a claims-made insurance policy?

- A. Insurance for claims and lawsuits initiated by the insured/policy holder.
- B. Liability insurance for lawsuits and demands made against the insured during the policy period.
- C. Insurance for losses that occur during the policy period.
- D. None of the above.



Answer to Polling Question #2

B. Liability insurance for lawsuits and demands made against the insured during the policy period.



Available First-Party Cyber Coverages

- Breach Response
 - Legal representation, computer forensic professional fees, notification costs, credit monitoring for affected individuals.
- Cyber Extortion Expenses
 - Professional fees to respond to ransom-type attacks, ransom payment.
- Business Interruption Costs
 - Lost profits attributable to network failure or interruption, may also include standard operating expenses, including payroll.



Available First-Party Cyber Coverages (cont.)

- Digital Asset Restoration
 - Costs and professional fees to restore or replace assets to *ex ante* status. Does not include costs to improve systems.
- Funds Transfer Fraud
 - Direct loss.
- Crisis Management Costs
 - Professional fees for public relations or crisis management consultants and direct costs for their work (e.g., media buys, notification costs).



Polling Question #3

Consequences of a data breach may include:

- A. Civil litigation.
- B. Mandatory provision of credit monitoring for affected customers.
- C. Regulatory and law enforcement investigations, proceedings, fines, and penalties; necessary technical costs to remediate network.
- D. All of the above.

Answer to Polling Question #3

D. All of the above.



Available Third-Party Cyber Coverages

- Network and Information Security Liability
 - Expenses and damages for claims arising from security failures, data breaches, and breach notice laws.
- Regulatory Defense and Penalties
 - Coverage for costs to comply with regulatory proceedings and fines.
- Multimedia Content Liability
 - Liability arising from dissemination of digital media content (e.g., slander, libel, violation of privacy, plagiarism, infringement of copyright and trademark).
- Merchant Services Agreement Liability
 - Sums owed to payment card companies or processors as a result of data breaches or security failure.



Cyber Insurance Claim Considerations

- Selection of Counsel and Panel Considerations
 - Best practice is to have breach counsel and forensic services firms in mind and approved by carrier as a matter of course – perhaps during underwriting process.
 - Carriers often have group of pre-approved counsel and remediation firms listed in policy itself, but these can present drawbacks.
- Notice of Claim
 - Check on policy to determine whether pre-notice costs are covered.
- Provide Notice to All Carriers – Not Only Cyber Insurer

Questions?



HODGSON RUSS

Contact Me



RYAN K. CUMMINGS

Partner

rcumming@hodgsonruss.com

716.848.1665

Anatomy of a Breach and Incident Response Planning



January 24, 2024
Patrick E. Fitzsimmons
Alexandria N. Rowen



Overview

- Current Trends.
- Types of Cyber Incidents.
- Responding to a Cyber Incident – Ransomware Attack.
- Importance of Incident Response Plan/Education and Training.



Current Trends

- Cybercrime is up approximately 600% since the COVID-19 pandemic.
- Experts predict that cybercrime will cost the world \$10.5 trillion annually by 2025.
 - The current estimate is \$6 trillion per year.
- Small businesses spend on average \$120,000 to \$1.24 million on a data breach.



Current Trends

USD 4.45M

Global average total cost of a data breach

33%

Only one-third of breaches were identified by the organizations' internal security teams and tools

277 days

Time to identify and contain a data breach

USD 250,000

20% of organizations that experienced a data breach paid this much or more in fines

Cost of a Data Breach Report 2023 – IBM Security



Polling Question #1

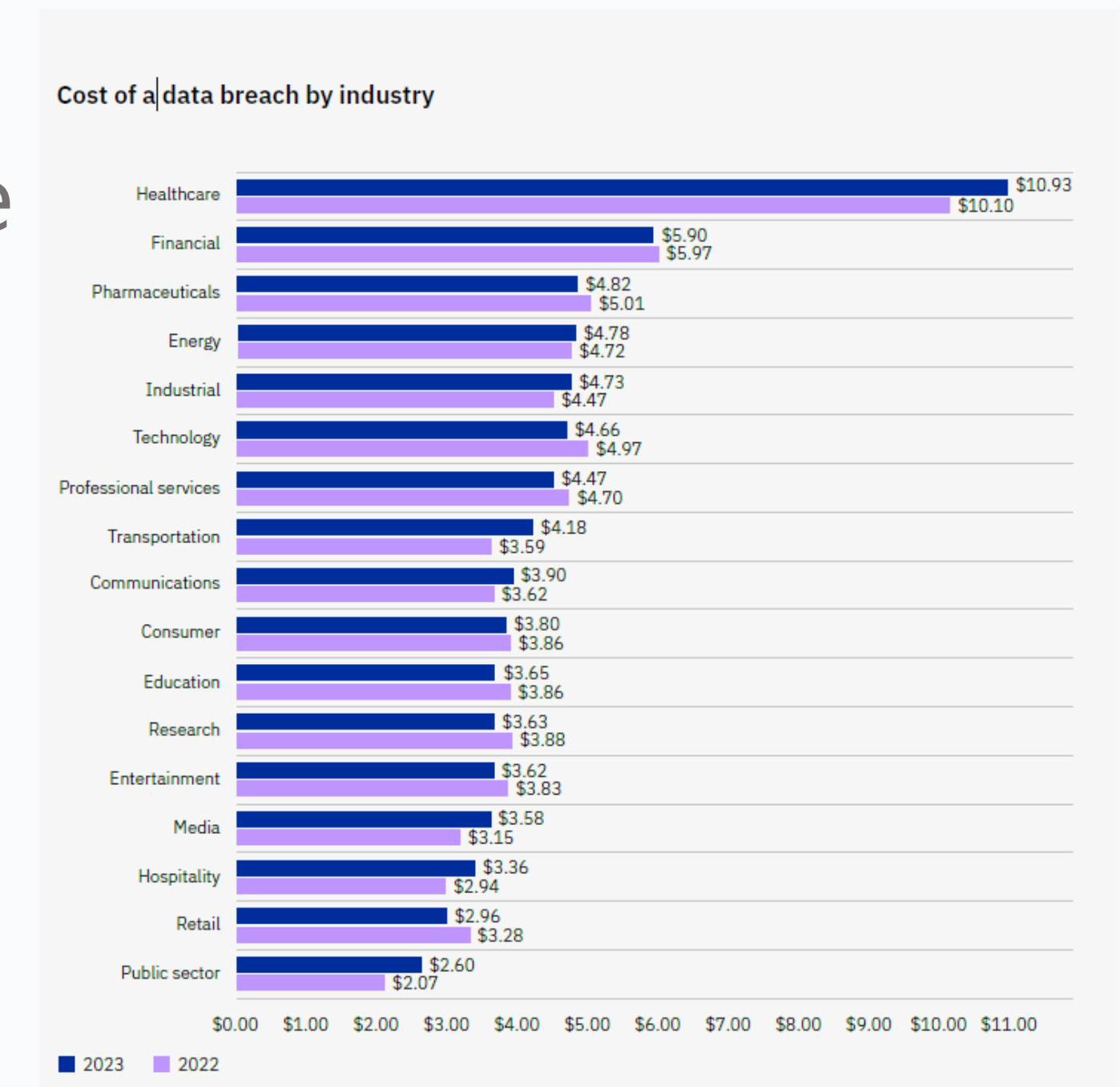
What industry experienced the highest data breach costs in 2023?

- A. Pharmaceutical Industry
- B. Healthcare Industry
- C. Financial Industry
- D. Energy Industry



Polling Question #1

- Answer: B. Healthcare Industry
 - Data breach costs in the healthcare industry hit \$10.93M in 2023
 - The remaining answers take the spots two through four on the list
 - Financial \$5.9M
 - Pharmaceuticals \$4.82M
 - Energy \$4.78M



Cost of a Data Breach Report 2023 – IBM Security



Phishing – What is it?

- Bad actors send emails that look credible to induce people to provide credentials and personal information.
- No longer are phishing emails easy to spot; they are more sophisticated and well written now and coincide with current events (*e.g.*, shipping notifications around the holidays; notices regarding tax season or elections).
- Phishing emails often contain links to click or attachments to “unlock” with credentials that the bad actors steal.

Phishing (Cont.)

- In 2023, the average cost of a data breach with phishing as the initial attack vector was \$4.76 M.
- Phishing was the most common attack vector and second most expensive in 2023.



Cost of a Data Breach Report 2023 – IBM Security

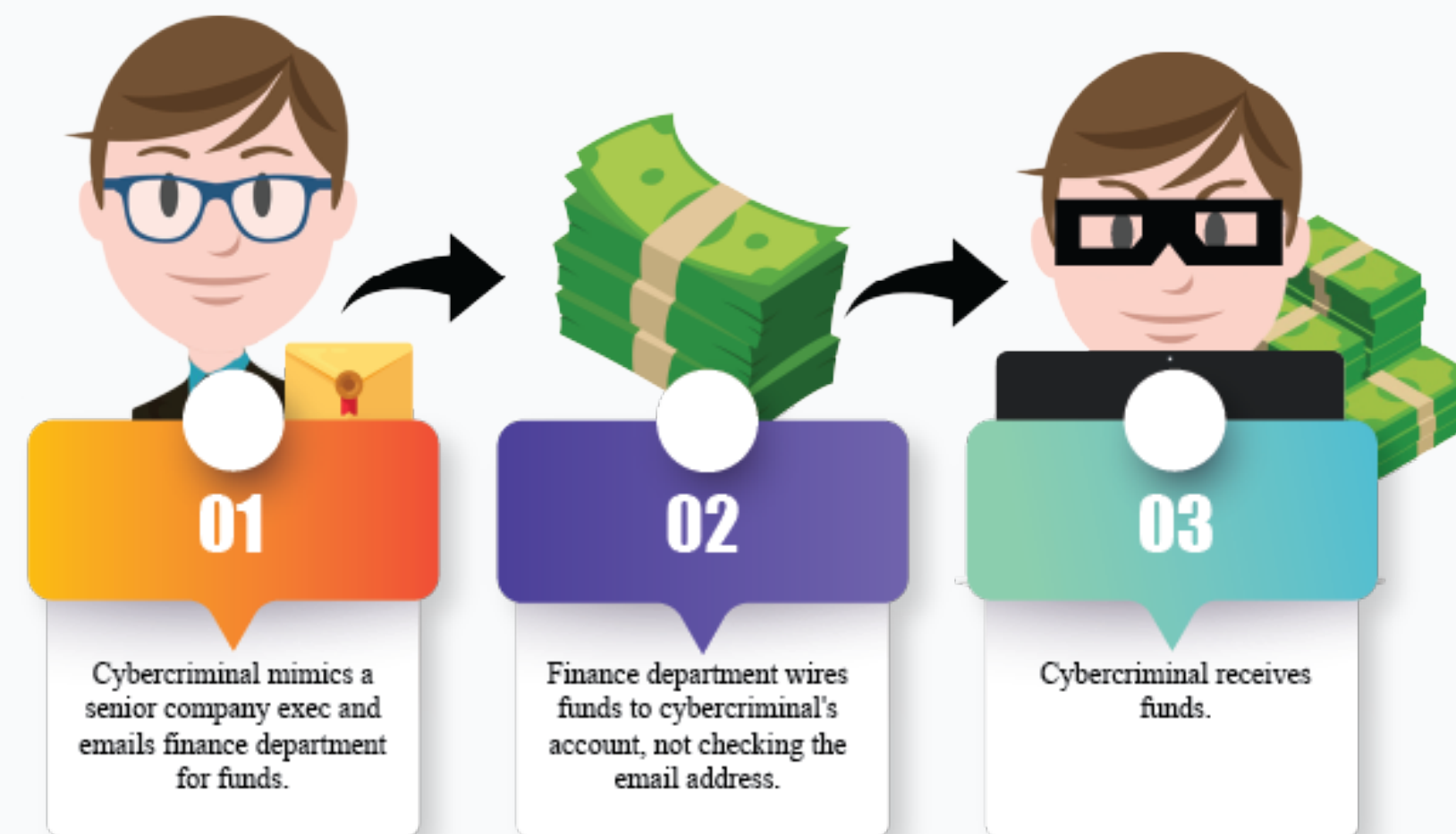


Business Email Compromise – What is it?

- Bad actor sends email impersonating someone (*e.g.*, financial officer of a company; a participant to a transaction) in order to dupe another party into sending funds to a “new” bank account controlled by the bad actor.
- The bad actor has either gained access to one of the transaction participants’ accounts or registered a domain name nearly identical that is hard to decipher.
 - pfitzsimmons@hodgsonruss.com vs pfitzsimmons@hogdsonruss.com
- The bad actor often does research on the company and knows who the relevant people are and/or that a transaction is about to close.
- Sometimes the bad actor has email account access for weeks or months, gains intelligence and waits for the right time to send the email catching everyone off-guard.

Business Email Compromise (Cont.)

- According to the FBI, there is a significant spike in this activity.
- In 2023, Business Email Compromises were the third costliest attack vector at \$4.67M.





Ransomware – What is it?

- Malicious software used to block access to computer systems and files.
- Malware infects systems and encrypts data following infiltration by, for example, a successful phishing or brute force attack.
- Bad actor demands payment in exchange for a decryption key/return of data.

XINOF v4.4.1



All Of Your Files Have Been Encrypted By XINOF!

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email to bds24@tutanota.com

XINOF

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us. After payment we will send you the decryption tool.
You have to 48 hours(2 Day) To contact or paying us After that, you have to Pay **Double**.
in case of no answer in 6 hours email us at = bds24@ProtonMail.com
The crypter person username : [bds24](#)
your SYSTEM ID is : [FDC9B3EA](#)

06d,20:58:25 ⚠

Attention!

- **DO NOT** pay any money before decrypting the test files.
- **DO NOT** trust any intermediary, they wont help you and you may be victim of scam. just email us , we help you in any steps.
- **DO NOT** reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.

What is our decryption guarantee?

- Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

You only have LIMITED time to get back your files!

- if timer runs out and you dont pay us , all of files will be DELETED and your hard disk will be seriously DAMAGED.
- you will lose some of your data on day 2 in the timer.
- you can buy more time for pay. Just email us .
- THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)

Regards- FonixTeam



Ransomware (Cont.)

- Ransomware attacks account for 24% of malicious attacks.
- Average cost of a ransomware attack is \$5.13M - an increase of 13% from 2022.
- Data exfiltration is more prominent now than in years past when encryption was the game plan.



Polling Question #2

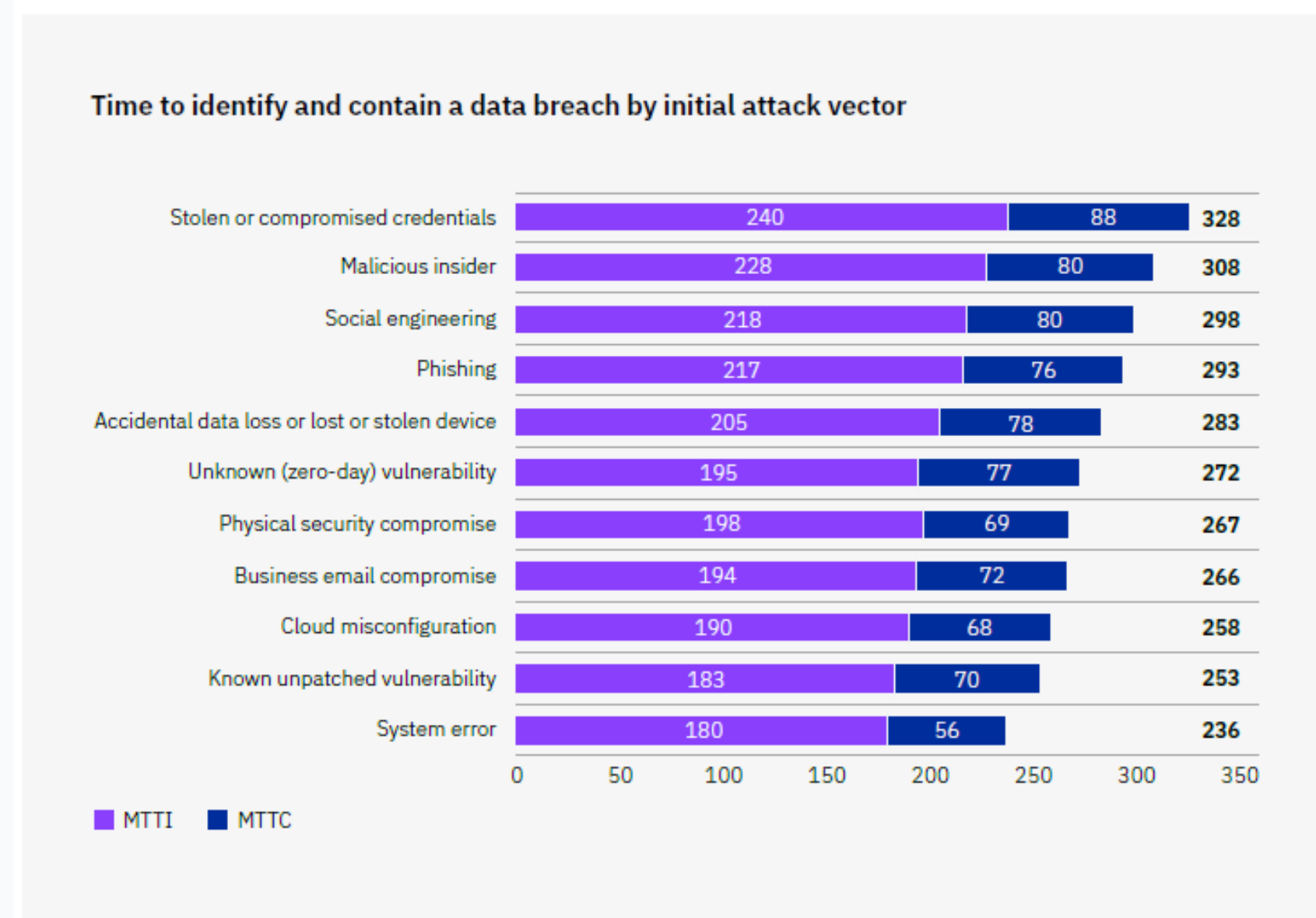
How long does it take to identify and contain data breaches resulting from stolen or compromised credentials?

- A. 8 months
- B. 6 months
- C. 1 month
- D. 11 months



Polling Question #2

- Answer: D. 11 months (328 days)
 - Average time to identify and contain data breaches will depend on the type of initial attack vector
 - Phishing = 293 days
 - Business Email Compromise = 266 days





Incident Response – Ransomware

Not a matter of “if” but “when”

Effectively there are three phases of work associated with responding to a cyber incident.

- Phase I – Discovery/First Days.
- Phase II – Negotiation/Analysis of Affected Data.
- Phase III – Notifications to Regulators/Affected Persons and Post-Incident Efforts.



Phase I – Discovery/First Days

- Company is hit with a cyber attack
 - Computers are locked down.
 - Ransom note provided.
- Cyber criminal can:
 - Make changes that affect the system's operation.
 - Disrupt normal business operation.
 - Exfiltrate data/information.



Phase I – Discovery/First Days (Cont.)

- What steps need to be taken?
 - Notify insurance carrier if coverage is in place.
 - Notify counsel.
 - Counsel will engage Forensic IT and/or ransom negotiator on behalf of company.
 - Protects privilege.
 - Forensic analysis begins
 - Determine what devices/networks affected.
 - Segregate affected network devices.
 - Assess back-ups.
 - Can the business restore and continue operations?
 - Regular calls with key players to discuss status of forensic analysis.



Phase I – Discovery/First Days (Cont.)

- Begin analyzing the affected data to determine scope
 - What devices were impacted and what data was there?
 - Isolation and mining the affected data.
 - Begin reviewing the affected data to determine data elements (*e.g.*, name, SSN, driver's license, financial information, health information).
 - Must understand what laws govern the business – regulator notices?
- Contact law enforcement
 - FBI – Internet Crime Complaint Center (IC3).
 - FBI does not intervene and take over negotiation on company's behalf but does share information regarding the bad actor.
 - FBI will recommend against paying ransom.
 - FBI sometimes has a decryption key that can be used.

Phase II – Negotiations/Analysis

- Ransom negotiator in contact with the bad actor
 - Back and forth on ransom amount.
 - Request/receive evidence of any exfiltrated data.
- Should the company pay the ransom?
 - Consider impact on:
 - Company culture.
 - OFAC Sanctions List.
 - Amount sought.
 - Whether any data was taken.
 - Can we restore from back-ups or are those also encrypted?
- Whether, and in what scenarios, a company will pay a ransom is something a company should discuss well before a breach happens.



Phase II – Negotiations/Analysis (Cont.)

- Forensic IT prepares written report
 - Report is prepared for counsel to protect privilege.
 - Report details what occurred – i.e., when bad actor first gained system access, how that occurred, what systems/networks/devices affected, exfiltration of data (if any), etc.
- Continued analysis of affected data
 - Begin identifying individuals affected by the breach and in what states they are located.
 - Does the data relate to people outside the US (e.g., Canada; EU)?
 - Need this information to determine if there is a reportable “breach.”



Polling Question #3

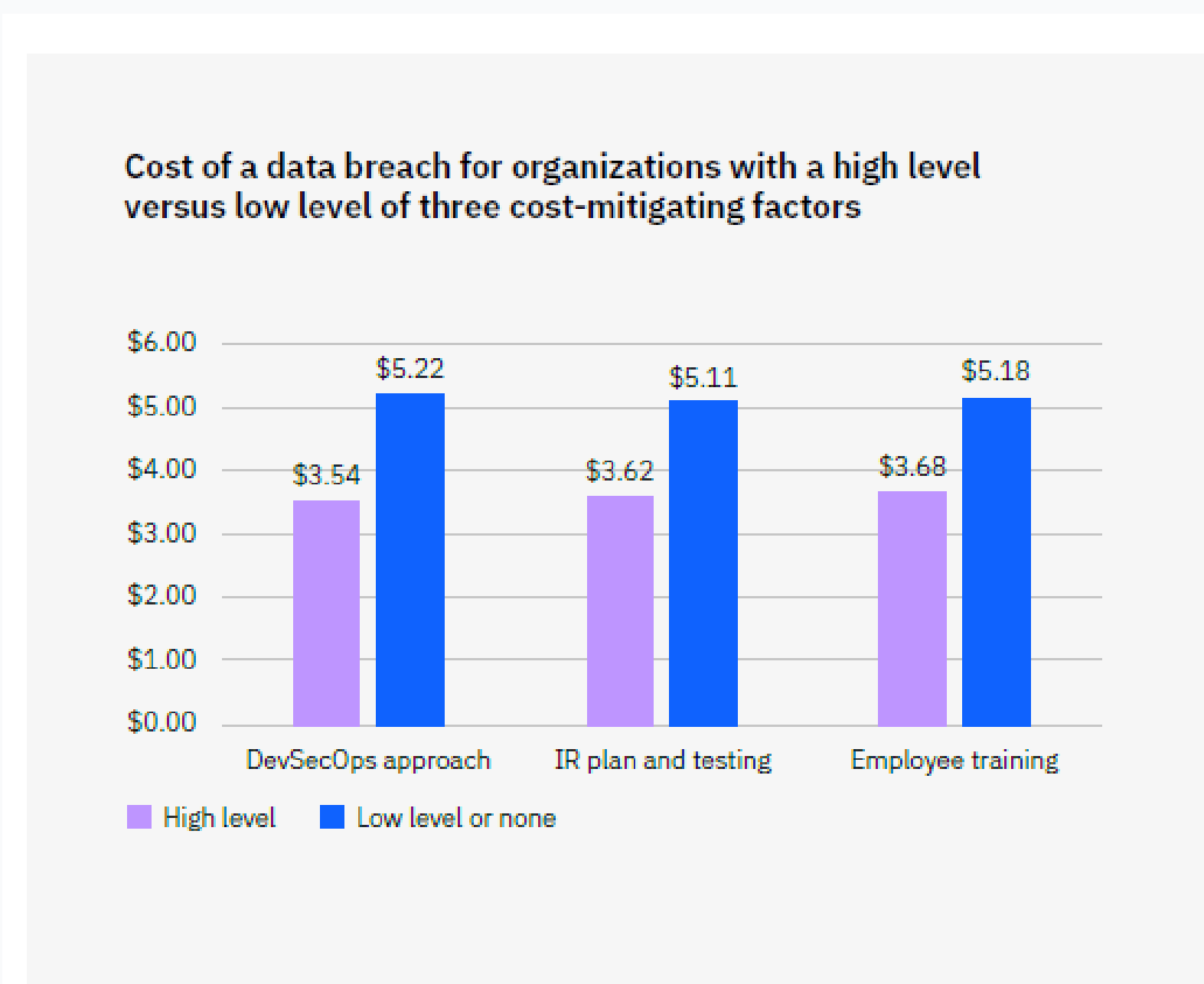
How much can companies save on a data breach with IR planning and testing?

- A. \$550,000
- B. \$1,000,000
- C. \$1,490,000
- D. \$2,100,000



Polling Question #3

- Answer: C. \$1,490,000
 - Organizations with cost mitigators, such as IR planning and testing, had significantly lower average costs of a data breach.





Phase III – Notifications

- Depending on the analysis, notification to affected individuals and regulators may be required.
- This requires an analysis of whether “personal information” was compromised.
 - Definition of personal information will depend on the state.
 - 50 US states with 50 different laws.
 - Generally speaking there are “access” states and “acquisition” states.
 - Typically, PI consists of first name or first initial with last name, along with:
 - Social security number
 - Driver’s license number
 - Financial account information
 - Biometric data
 - Etc.



Phase III – Notifications (Cont.)

- Must determine where affected individuals are located.
 - Vendors can assist with obtaining this information.
- Notification will typically depend on whether information was accessed or acquired.
- Some states may require notice to regulators.
- Notice is typically required in the most expedient time possible or without undue delay.



Phase III – Notifications (Cont.)

- Content of notification letters depends on each state's law but generally includes:
 - Date of the security breach.
 - General description of the breach.
 - Personal information affected by the breach.
 - Contact information for the entity.
 - Contact information for major consumer reporting agencies and local law enforcement or regulatory authorities.
 - Advice to recipient to review personal account statements and credit reports.



Phase III – Notifications (Cont.)

- Some states require credit monitoring or identity theft protection services.
 - Credit monitoring = basic.
 - Only monitors credit reports.
 - *E.g.*, Massachusetts (18 months).
 - Identity theft protection = robust.
 - Monitor credit reports, look for fraudulent purchases or activity, search dark web for personal information, etc.
 - *E.g.*, Connecticut (24 months).
- After notifications are sent, the company should be prepared to answer questions if/when contacted by individuals/regulators.
- After a cyber incident the company should conduct a post-mortem exercise and review what happened, come up with lessons learned, and amend their policies and procedures as necessary to be more prepared in the future.



Is Your Company Ready for a Breach?

- Incident Response Plan in Place.
- Proper Insurance Coverage.
- Training/Education of Employees.
- Enable Multifactor Authentication.
- Perform Penetration Testing.
 - Assess vulnerabilities in systems to appropriately safeguard.
- Tabletop Exercises – practice various scenarios and establish muscle memory.
- Recovering From a Cyber Incident:
 - Use safe backups to resume operations.
 - Recover or rebuild the lost data.
 - Conduct a post-mortem analysis to learn from the incident.
 - Analyze and improve your cybersecurity procedures and policies.



Example Tabletop Exercise

Potential Business Email Compromise:

Late Friday afternoon, the IT help desk is contacted by an employee working on a transaction who says the other parties informed him they received suspicious emails containing wiring instructions related to the deal that appear to come from his email address. The employee also says that he recently received a suspicious email that turned out to be a phishing email where he entered his credentials, but because he was busy, he forgot to notify IT.

- How would your team assess this?
- Who at your company needs to be informed?
- Who at your company needs to be involved?
- What are the next steps from there?

Questions?



HODGSON RUSS
Contact Us



PATRICK E. FITZSIMMONS

Partner

pfitzsim@hodgsonruss.com

716.848.1710



ALEXANDRIA N. ROWEN

Associate

arowen@hodgsonruss.com

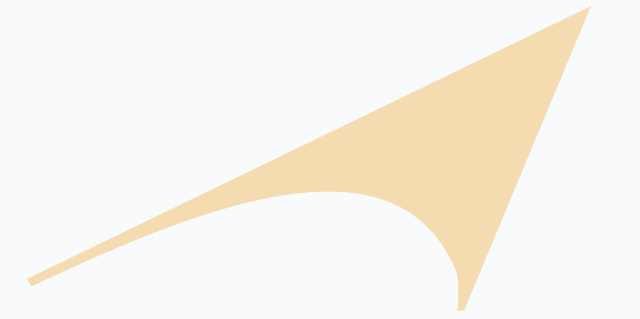
716.848.1759

Vendor Contracting Practices as Risk Mitigation: Data Privacy Considerations



January 24, 2024
Gary M. Schober
Rosellen D. Marohn

Vendor Engagement



- Engagement of vendors that have broad access to company systems and data is an inevitable reality (e.g. Microsoft Office 365, SalesForce, ADP).
- Safely engaging vendors that access, process or host sensitive or confidential organizational data, including employees' and customers' personal information, should be actively managed.
- Doing so requires specific attention and oversight to comply with applicable laws, regulations and industry standards.

Organizational accountability cannot be outsourced!



Establishing a Privacy and Data Security Focused Vendor Management Process

- Perform pre-engagement (or pre-agreement renewal) vendor due diligence.
- Develop and implement standard contractual terms/forms that address your organization's privacy and information security requirements.
- Practice regular vendor oversight and contract enforcement.

Pre-Engagement Due Diligence



- Identify the service to be performed and what access is required by the vendor to perform the services (e.g. IT systems, proprietary data, personal information, etc.). Keep the “minimization rule” in mind.
- Evaluate if vendor’s proposed access to proprietary and personal information or systems can be reduced without diminishing the services to be provided.
- Evaluate the vendor’s policies, procedures, internal controls and certifications.
- Review the vendor’s privacy and data security history along with performing general due diligence (e.g. litigation, data breaches, regulatory actions, etc.).

Key Questions to Ask of Potential Vendors



- Consider if developing a vendor assessment questionnaire or checklist with targeted privacy and data security questions or key topics for review would be valuable to your organization.
- How does the vendor intend to perform the proposed services?
- Does the vendor currently comply with applicable laws, regulations, industry standards, etc.?
- Review the vendor's privacy and information security policies and protocols. A privacy policy should be required.
- Request copies of results from data security risk assessments such as penetration tests and remediation plans.
- Request details of any past incidents or data breaches.



Polling Question

Does your organization have an established procurement process when engaging outside vendors that will have access to your organization's data?

- A. Yes
- B. No
- C. Sort of

Special Considerations – Artificial Intelligence



- Risks of AI use:
 - Privacy
 - Intellectual Property
 - Bias
 - Hallucinations
- Develop standard questions for vendors around the use of AI
 - What type of AI is used in the relevant product/service?
 - How will your entity's data be used with respect to AI? What licenses to data are you granting?
 - What rights do you have to input/output data?

Vendor Certifications



- Based on organizational needs, consider requiring third-party assessments, audits or certifications.
- Consider requiring specific technical risk assessments such as penetration tests or vulnerability scans.
- Consider third-party certifications as may be appropriate based on industry:
 - Service Organization Control (SOC) Reports, e.g. SOC 2 (privacy and data security controls).
 - ISO 27001 Certification.

Contract Review and Drafting – Minimum Standards



- Develop standard privacy and security contracts that:
 - Meet or exceed your organization's own practices.
 - Adhere to your organization's policies and procedures.
 - Comply with applicable laws, regulations and industry standards.
 - Provide rights to assess and review vendor's compliance, including audits.

Contract Review and Drafting – Minimum Standards (Cont.)



- Consider if it makes sense to prohibit:
 - selling or sharing personal information.
 - retaining, using or disclosing personal information for any purpose other than for the business purposes specified in the contract.
 - retaining, using or disclosing the information outside of the direct business relationship between the service provider/contractor and the business.
 - combining the personal information it receives under the contract with personal information it receives itself or from other entities.

Vendors often prefer to use their own vendor-friendly documentation – beware!



Polling Question

Does your organization use artificial intelligence in your day-to-day business operations?

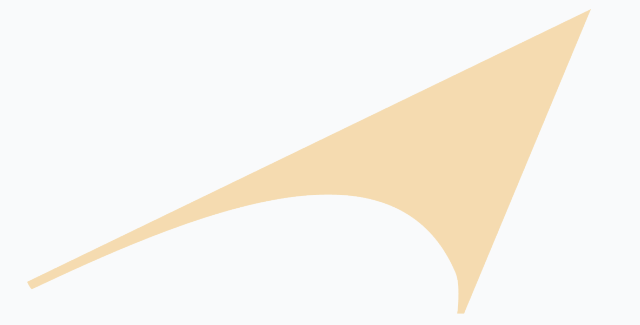
- A. Yes
- B. No
- C. Maybe

Data Processing Agreements (DPAs)



- Data Processing Agreements, also commonly referred to as Data Processing Addendums.
 - May be applicable when engaging third-party vendors or when acting as third-party service provider.
 - Address privacy and data security obligations.
 - Often incorporated by reference into MSAs, Enterprise Agreements, SaaS Agreements, etc.
- DPAs are becoming increasingly more common.
 - Growing number of data privacy laws, particularly in the U.S.
 - Globalization of services.
 - Proliferation of “as a Service” business model, such a SaaS, DaaS, XaaS.
- Often drafted to address specific data privacy laws (most often GDPR, UK GDPR, CCPA/CPRA). Catch-all language such as “as may be amended from time to time” and “all other applicable data privacy laws” are often included.

Is a DPA Really Necessary?



- When engaging third-party vendors, the necessity of a DPA most usually requires a case-by-case analysis.
- Do industry specific data laws apply to your operations?
 - Gramm-Leach-Bliley Act (Financial Services).
 - HIPAA (Healthcare).
 - FERPA (Students/Education).
- What data will be involved in the vendor engagement?
- Who are the data subjects and where are they located?
What geographically specific laws apply?
- Where and how will the data be transferred?

Risk Allocation

- Consider indemnification provisions and limitations on liability.
- Requirement of cyber or other forms of insurance.
- Be cognizant of how regulatory penalties or other liability related to failure to meet privacy and data security requirements, data breaches or other cybersecurity incidents are addressed.

Negotiations

- Conduct an RFP process when possible.
- Negotiate privacy and data security terms in conjunction with pricing and other business terms.
- Use caution when using vendor-provided agreements.
- Leverage publicly disclosed cyber vulnerabilities and incidents.



Polling Question

- How often does your organization audit its relationship with key vendors?
 - Annually
 - Upon contract renewal
 - When there's an issue
 - Almost never

Oversight and Enforcement



- Monitor vendor performance and compliance with contract terms.
- If risks or potential issues are identified, address them as soon as practicable to avoid larger problems.
- When business relationships end, ensure data is returned by vendors, destroyed or otherwise protected.
 - In today's environment, return or destruction of data isn't practical or possible due to the need for back-up copies (ex. on servers or in the cloud).
- Consider conducting onsite visits or requiring third-party audits, etc.

Continual Monitoring



- Make privacy and data security a priority! It's here to stay and only growing more prevalent.
- With periodic regularity, review legal developments with respect to cybersecurity and privacy.
- Update standard language and forms to account for any developments that may be applicable to your operations.
- Consider the need for agreement amendments or restatements for already existing agreements.
 - Develop a targeted approach, addressing mission critical and high impact agreements first.

Questions?



HODGSON RUSS
Contact Us



GARY M. SCHOBER

Partner

gschober@hodgsonruss.com

716.848.1289



ROSELLEN D. MAROHN

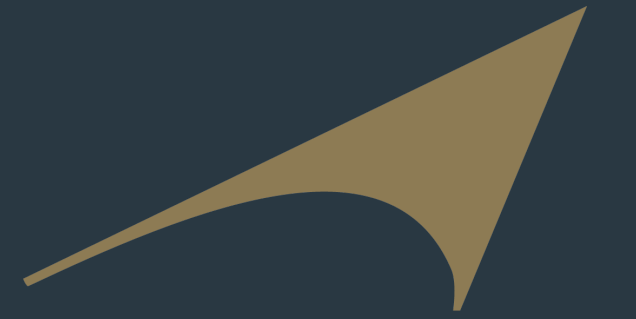
Associate

rmarohn@hodgsonruss.com

716.848.1414

HODGSON RUSS

Disclaimer



This presentation is intended for general informational purposes only and does not constitute legal advice or legal opinion on any specific facts or circumstances. Information contained in this presentation may not be appropriate to your particular facts or situation. You should not act upon the information in this presentation without consulting Hodgson Russ LLP or other professional advisors about your particular situation. No attorney-client relationship with Hodgson Russ LLP is established by viewing this presentation. Hodgson Russ LLP makes no representations as to the accuracy or completeness of any information in this presentation, and the opinions expressed in this presentation are the opinions of the individual authors and may not reflect the opinions of the firm or any individual attorney.

All copyrightable text and graphics, the selection, arrangement, and presentation of these materials (including information in the public domain), are ©2024 Hodgson Russ LLP. All rights reserved. Permission is granted to download and print these materials for the purpose of viewing, reading, and retaining for reference. Any other copying, distribution, retransmission, or modification of these materials, whether in electronic or hard copy form, without the express prior written permission of Hodgson Russ LLP, is strictly prohibited.