



Cybersecurity Issues in the Hospitality and Retail Industry

A Survey of Technical Issues and Noteworthy Cases



Key Current Security Risks & Mitigation Approaches

Litigated Examples



Robert G. Smith
LORANCE THOMPSON, P.C.
Houston, Texas
rgs@lorancethompson.com
(713) 868-5560

Nobody is exempt...

- Marriott
- Facebook
- Uber
- Target
- Equifax
- Sep. 25, 2017 “*The Guardian* said a breach at Deloitte involved usernames, passwords and personal data on the accountancy’s top blue-chip clients...companies include household names as well as US government departments.”

What is Information Security?

Protects following characteristics:

- **Confidentiality** - Who can see the data?
- **Integrity** – Who can change the data?
- **Availability** – Ensuring that the data is available to authorized people.

Types of Threats

- IoT device malfunction
- Cyber-attack and theft of personal data stored on IoT
- IoT devices used to cause financial, physical, or political harm

Sources of Threats

Internal Threats

- Disgruntled Employees
- External Contractors
- Employees that are negligent, misinformed, or have made a mistake

External Threats

- Hackers
- Foreign Countries
- Corporate Spies
- Protesters
- Organized Crime

New Cyber Risks

- Duty to create products better than human
- Duty to recognize and intervene when software is malfunctioning
- Standard higher than reasonable person

Data Exhaust

- User information
- Location
- Preferences
- Financial information

Cyber Defenses

- Employee education
- Vetting of vendors/contractors
- Retrofitting
- Maintaining software updates

Litigation Defenses

- Preemption
- Learned Intermediary
- Contributory Negligence
- Intervening cause

Mitigation

- Include analog controls
- Insurance
- Cyber security plan
- Contractual provisions
- Regulations

Consequences of Security Breaches

Consequences

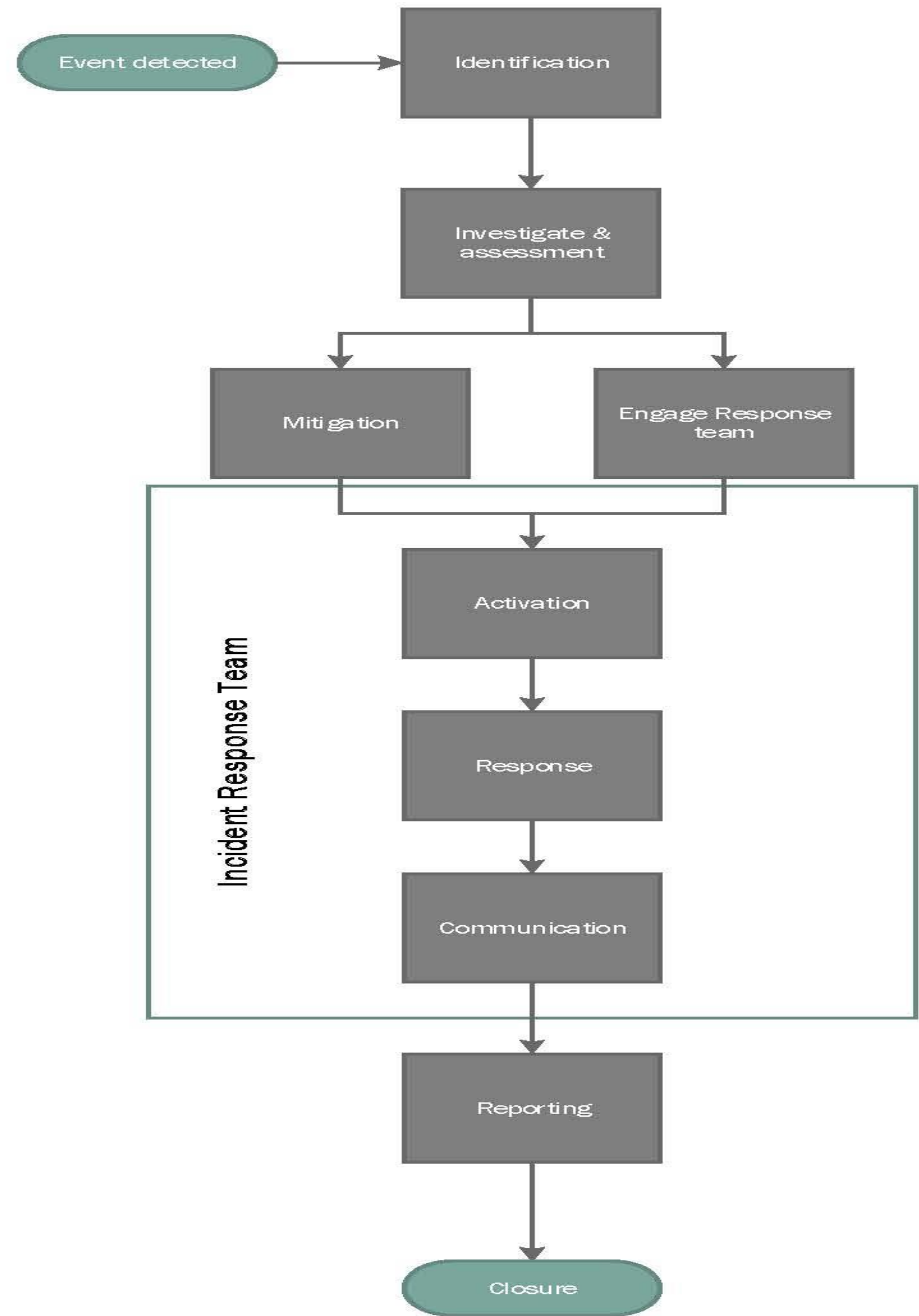
- **Confidentiality** - Risk to personal or confidential information.
- **Integrity** - Data corruption or destruction.
- **Availability** - Unavailability of business data or critical information in an emergency, etc. (Email, ERP, etc.)

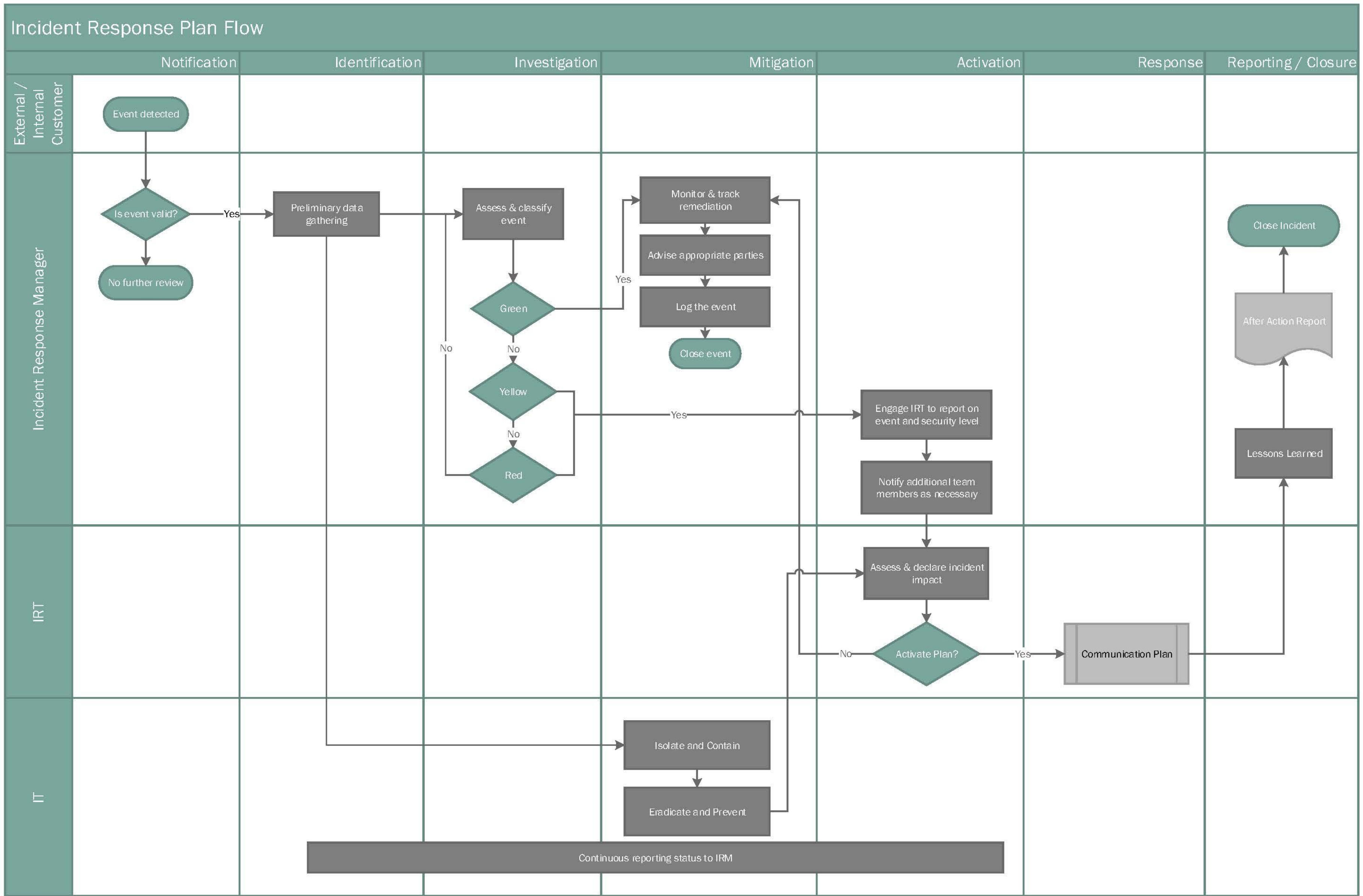
Other Consequences:

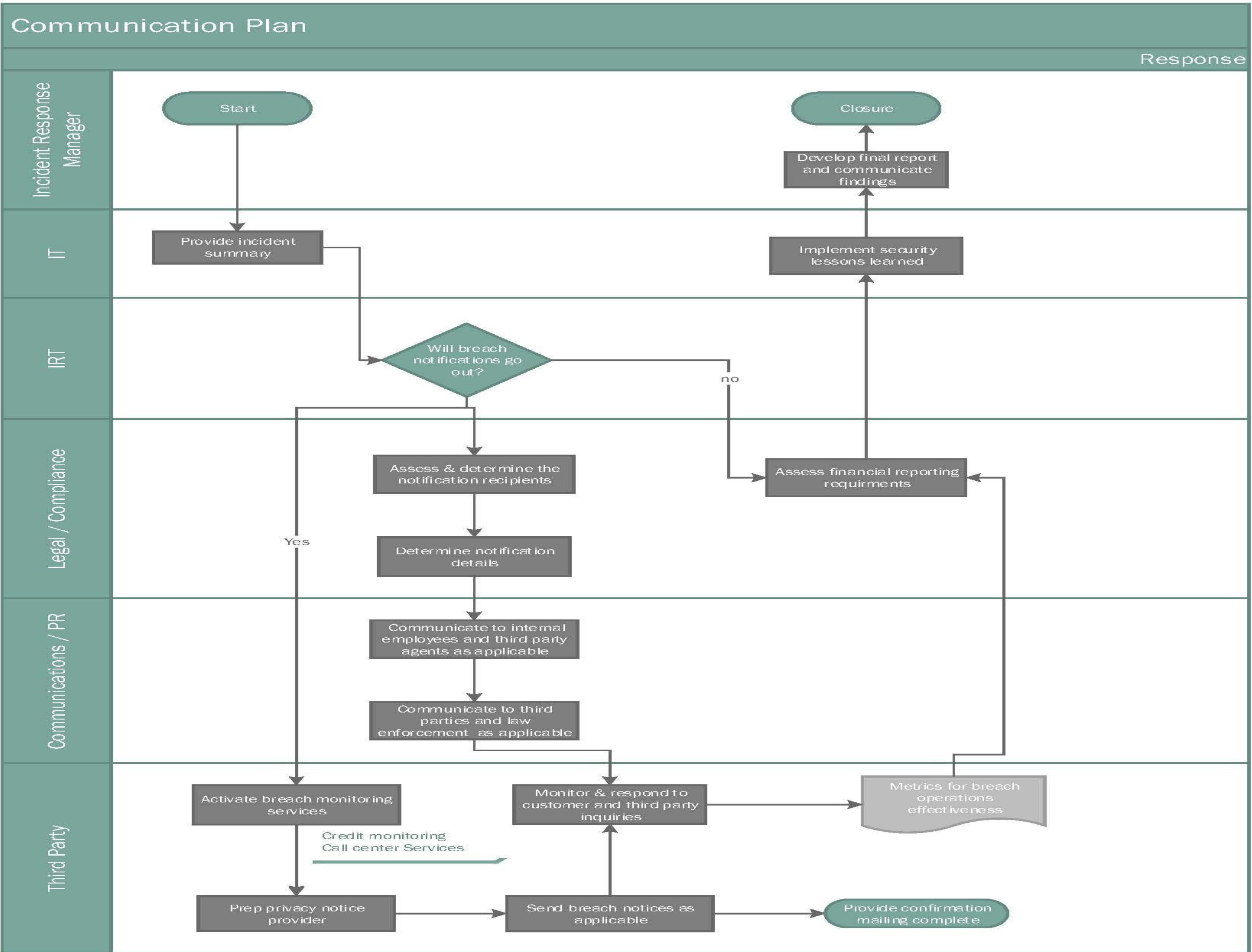
- Loss of trust from employees and the public.
- Impact on Brand.
- Costly reporting to the government and remediation requirements.
- Potential for large fines, penalties and lawsuits.

Cyber Security Plans

- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan










Data Breach Reporting Requirements



Jeremy Ward
**FRANDEN | FARRIS | QUILLIN |
GOODNIGHT + ROBERTS**
Tulsa, Oklahoma
jward@tulsalawyer.com
(918) 583-7129

State Reporting Requirements



Why are they important?

You will be targeted!

- In 2017, 7.8 billion records were exposed . . . an increase of 24.2% over 2016.
- Average cost of breach: \$7 million.

Why are they important?

- *So far in 2018:*

- Arby's
- Gamestop
- Kmart
- Whole Foods
- Sonic
- Forever 21
- Panera Bread
- Lord & Taylor
- Saks Fifth Avenue
- Best Buy
- Delta
- Sears
- Under Armour

Why are they important?

No business is too big or too small . . .

- **Equifax**

- Consumer credit reporting agency
- In 2017, experienced a data breach which affected 147.9 million consumers.
- Accessed consumer's names, Social Security numbers, birth dates, addresses, and driver's license numbers.

Why are they important?

No business is too big or too small . . .

- **Small Businesses**

- 50%-60% of small businesses will be breached this year.

Why are they important?

- State Attorney Generals are starting to get serious about enforcement of disclosure guidelines.
 - Pennsylvania Attorney General's Office has filed a lawsuit against Uber for violating Pennsylvania's breach notification law.
 - ***Seeking \$13.5 million in damages.***
 - West Virginia and Massachusetts Attorney Generals have filed lawsuits against Equifax based, in part, on a failure to quickly notify affected individuals.
 - ***West Virginia AG seeking \$5,000 per violation for each of the 730,000 violations.***

Which states are affected?

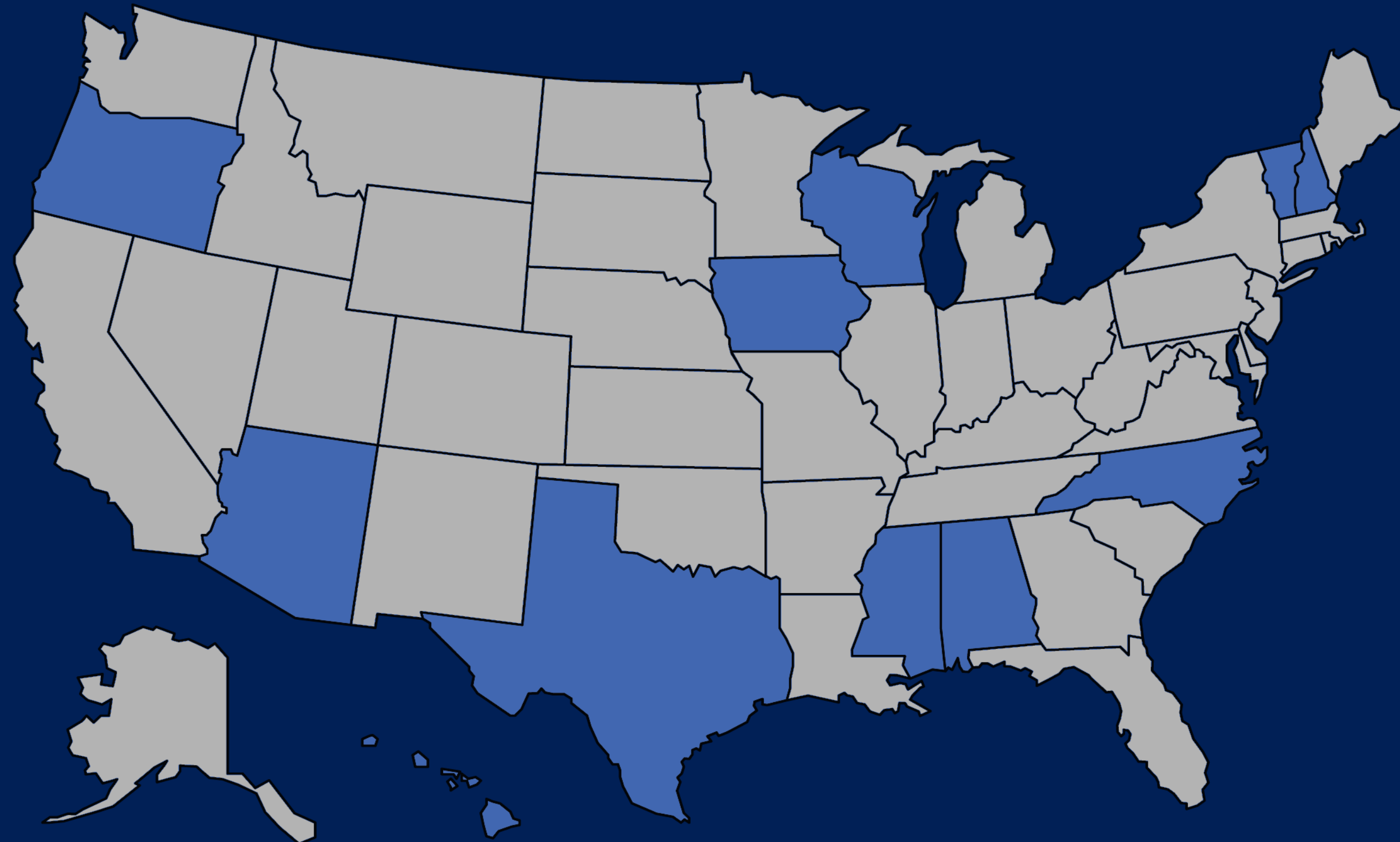
- All 50 states and the District of Columbia have passed legislation imposing reporting requirements.
- Laws vary as to who to report a breach to and when the breach must be reported.

Who must you report to?

- All states require businesses to notify the resident individuals affected by the breach.
 - Some states also require notification of the breach to nonresidents.

Who must you report to?

Some states
require notification
of all affected
individuals:

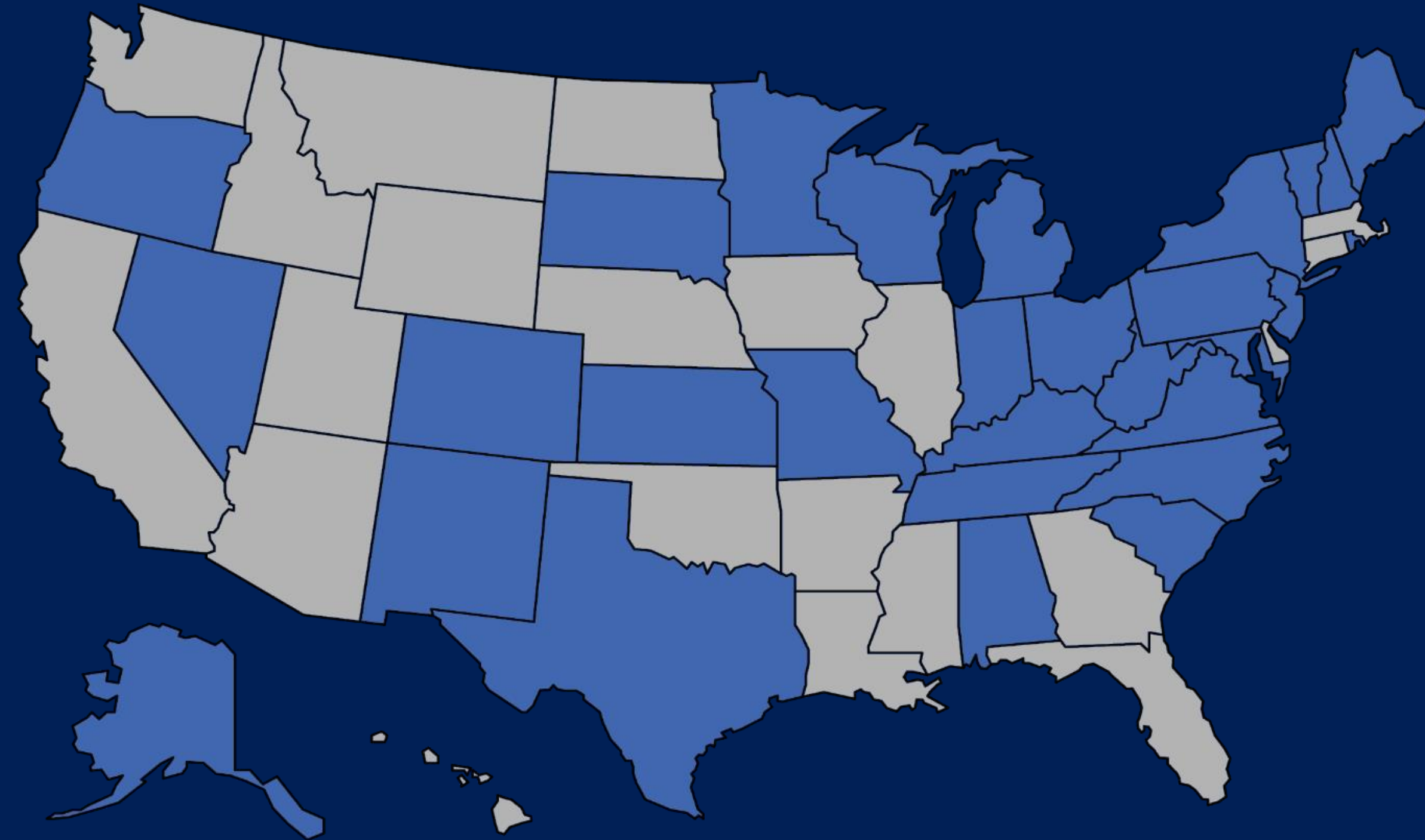


- All individuals regardless of residency

Alabama, Arizona, Hawaii, Iowa, Mississippi, New Hampshire, North Carolina, Oregon, Texas, Vermont, and Wisconsin

Who must you report to?

Credit Reporting Agencies

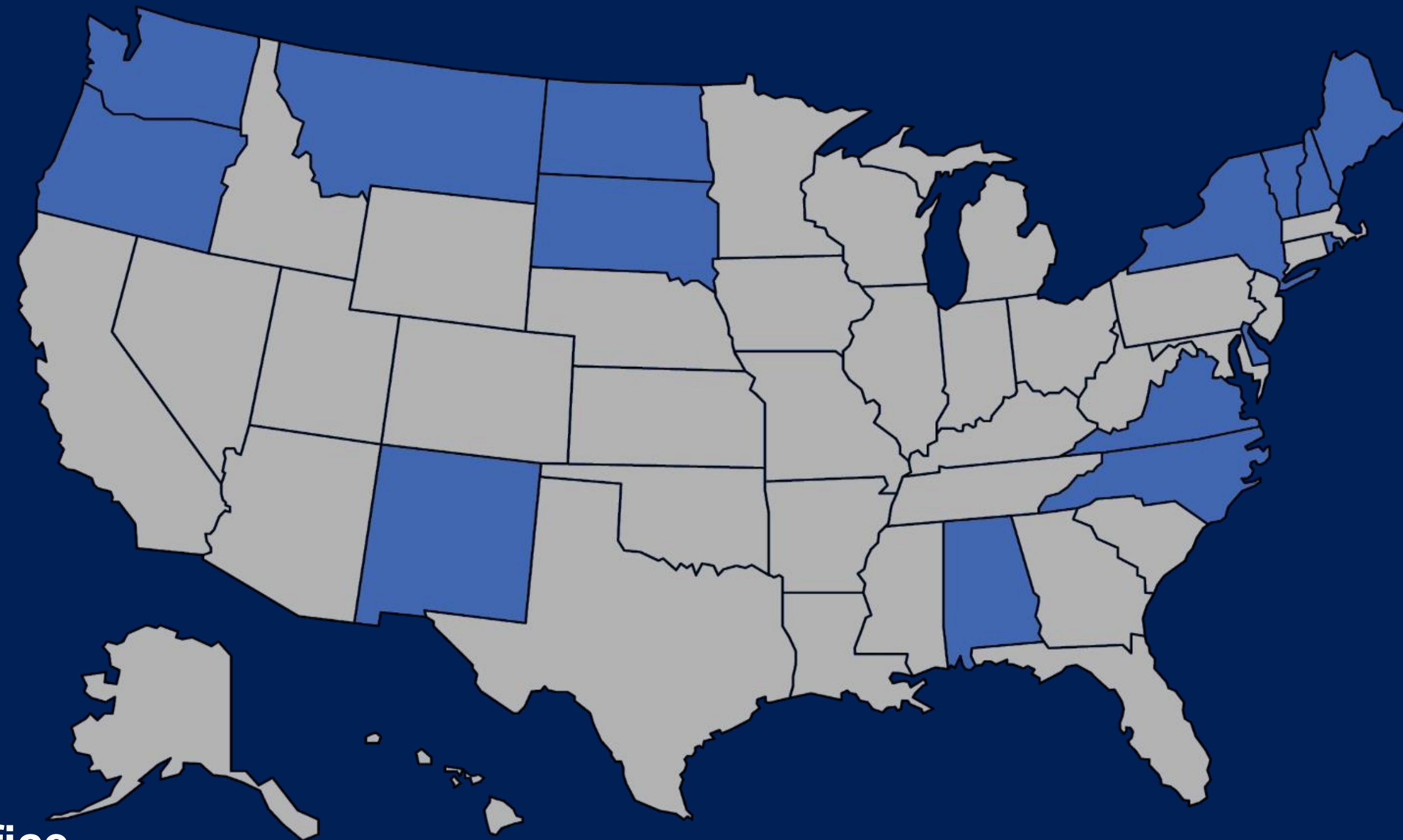


- **Notification to credit reporting agencies**

Alabama, Alaska, Colorado, Indiana, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, West Virginia, Wisconsin, District of Columbia

Who must you report to?

Attorney General's Office



- **Notification to Attorney General's Office**

Alabama, Delaware, Maine, Montana, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Dakota, Vermont, Virginia, Washington

Who must you report to?

Notify Additional Regulatory Agencies

- Maine – Appropriate state regulators in the Department of Professional and Financial Regulations
- New Hampshire – Regulators with primary regulatory authority
- Vermont – Department of Financial Regulation
- New Jersey – Division of State Police in the Department of Law and Public Safety

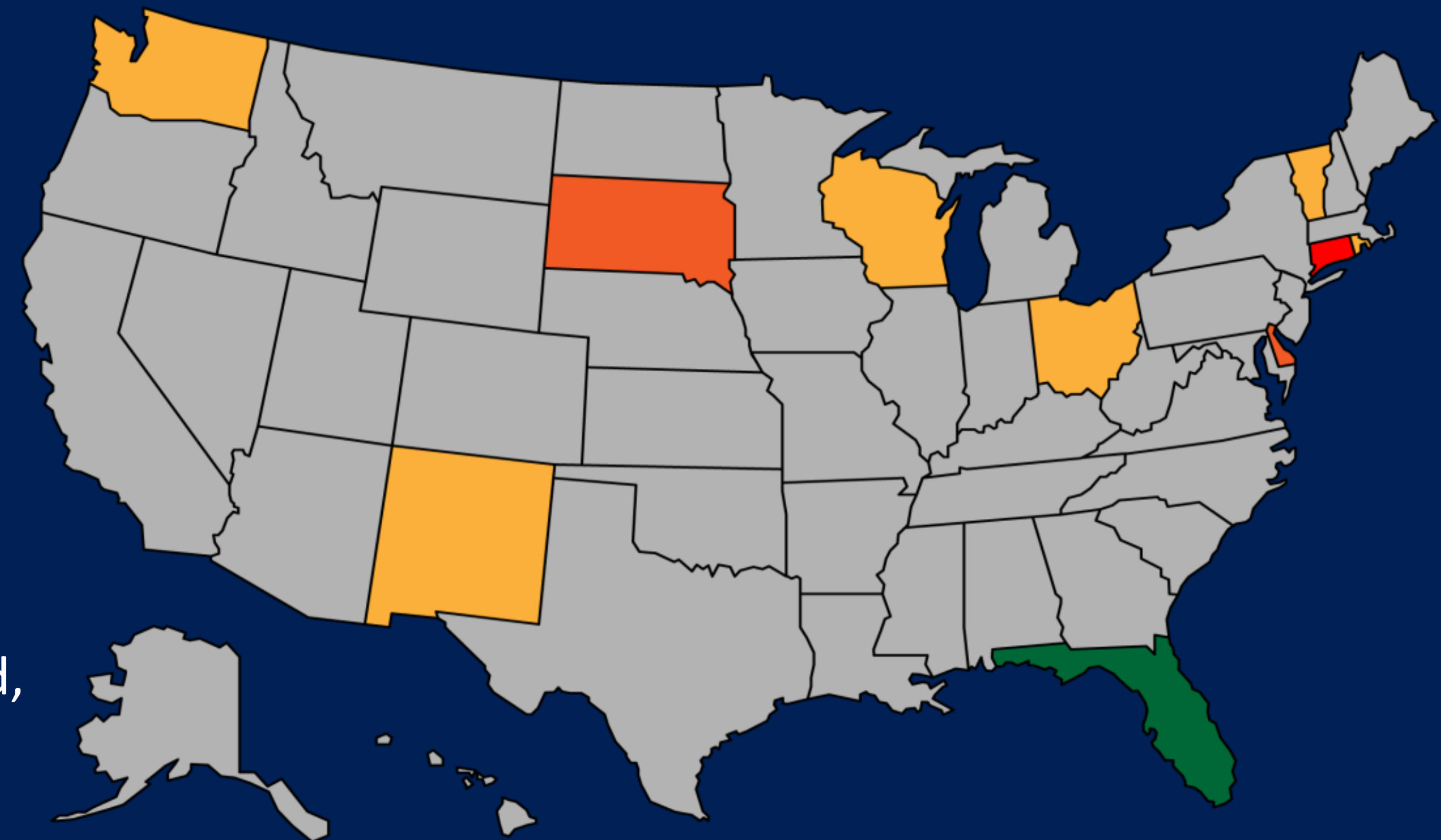


When must you report?

Most states require disclosures to be made “as expeditiously as possible” and “without unreasonable delay.”

Exceptions are:

-  **90 days**– Connecticut
-  **60 days** – Delaware, South Dakota
-  **45 days** – New Mexico, Ohio, Rhode Island, Vermont, Washington, Wisconsin
-  **30 days** - Florida



Reporting Requirements for Federal Contractors



Cybersecurity Risks

- Federal agencies are a prime target for hackers because a breach can expose both government information and citizens' personal identification information.
- 70% of federal agencies have been breached.
- 57% of federal agencies were breached in 2017.

Requirements for Contractors

- No uniform set of requirements for all federal contractors.
- Contractor requirements are
 - (1) Contract specific and
 - (2) Agency specific.

Federal Information Security Modernization Act

- In 2014, Congress passed an updated version of the Federal Information Security Modernization Act (“FISMA”).
- Purpose: to establish oversight and accountability for federal agencies.
- As part of FISMA, the Office of Management and Budget created a uniform policy and guidelines for all federal agencies.

Federal Information Security Modernization Act

- Agencies are to include terms in their contracts that will allow the agency to effectively address a data breach.
- Those terms include requirements that contractors:
 - “cooperate with and exchange information with agency officials...in order to effectively report and manage a suspected or confirmed breach”
 - “report a suspected or confirmed breach...as soon as possible and without unreasonable delay”

Federal Information Security Modernization Act

- What about notifying the affected individuals?

Agencies may, but do not have to, require contractors to notify all individuals affected by a data breach.

Federal Information Security Modernization Act

- **Department of Defense:**
 - Cyber incident: “actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein”

Federal Information Security Modernization Act

- **Department of Defense:**
 - Report to DOD within 72 hours of discovering that a cyber incident has taken place.
 - Report through *<http://dibnet.dod.mil>*

Federal Information Security Modernization Act

- **Department of Justice:**
 - Report within 1 hour of discovery.
 - Applies to a breach *or* attempted breach.
 - Report to Department of Justice Computer Emergency Readiness Team (“DOJCERT”); Contracting Officer; and Contracting Officer’s Representative.



OVERVIEW

LEGAL PERSPECTIVE

- What happens after the breach
- Proactive Pre-breach planning
- Post-breach execution of plan



Thomas A. Capezza
CARTER CONBOY
Albany, New York
tcapezza@carterconboy.com
(518) 465-3484



TODAY'S GOAL

- Sensitize you to legal issues that follow a breach
- Position you to address those legal issues

Prioritize Institutional Assets

- Determine which data, assets, and services warrant the most protection to keep the business functioning
- This will mitigate harm caused by a cyber intrusion

	Urgent	Not Urgent
Important	NOW	LATER
Not Important	DELEGATE	TRIVIAL

Have an Incident Response Plan Before an Intrusion Occurs

- Who has **lead responsibility** for different elements of incident
- Controlling **communications** – technical, legal, public relations
- Preserve data-related **priorities** consistent with business needs
- Preserve data, **logs**, in a forensically sound manner
- Criteria for **notifying** data owners, customers, and partner companies
- Procedures for notifying **law enforcement**

Pre-breach Planning – Incident Response Plan Guidance

National Institute of Standards and Technology

- NIST Cybersecurity Framework uses the **Identify, Protect, Detect, Respond,** and **Recover** language to express management of cybersecurity risk

FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	

Pre-breach Planning – Incident Response Plan Guidance

- **identify** internal and external cybersecurity risks threatening the security or integrity of non-public data stored on the entity's information systems
- use defensive infrastructure and policies to **protect** the entity's information systems and non-public data
- **detect** cybersecurity events
- **respond** to cybersecurity events to mitigate any negative effects
- **recover** from cybersecurity events and restore normal operations and services

System Assessment to Establish Baseline

- Overall system assessment
- Harden vulnerabilities
- Establish a baseline regarding system security
- Helpful to answer the legal question: **who is responsible for the consequences of the data breach – the hacker or the company that failed to ensure adequate security measures?**



System Monitoring and Authorization

- Technology resources in place before intrusion occurs
 - Back-up, intrusion detection, data loss prevention, filtering and scrubbing
- Authorization to notify users of collection, storing, and use of communications – e.g., banners
- Policies align concerning “insider threats”
- Engage law enforcement before an incident

Post-breach Execution – Incident Response Plan

Overview

- Make an Initial Assessment
- Implement Measures to Minimize Continuing Damage
- Record and Collect Information
- Notify

Post-breach Execution – Incident Response Plan

Make an Initial Assessment

- Nature and scope of the incident
- Malicious act or technical glitch
- Identify affected computers, origin of incident, malware, affected remote servers
- Identify any other victim organizations
- Evidence of intrusion including logging must be preserved
- Avoid modifying data



Implement Measures to Minimize Continuing Damage

- Reroute network traffic, isolating all parts of the compromised network
- Consider abandoning affected network and restoring with a backup
- Consider closing the ports being used to gain access
- Keep records of steps taken to mitigate



Post-breach Execution – Incident Response Plan

Record and Collect Information

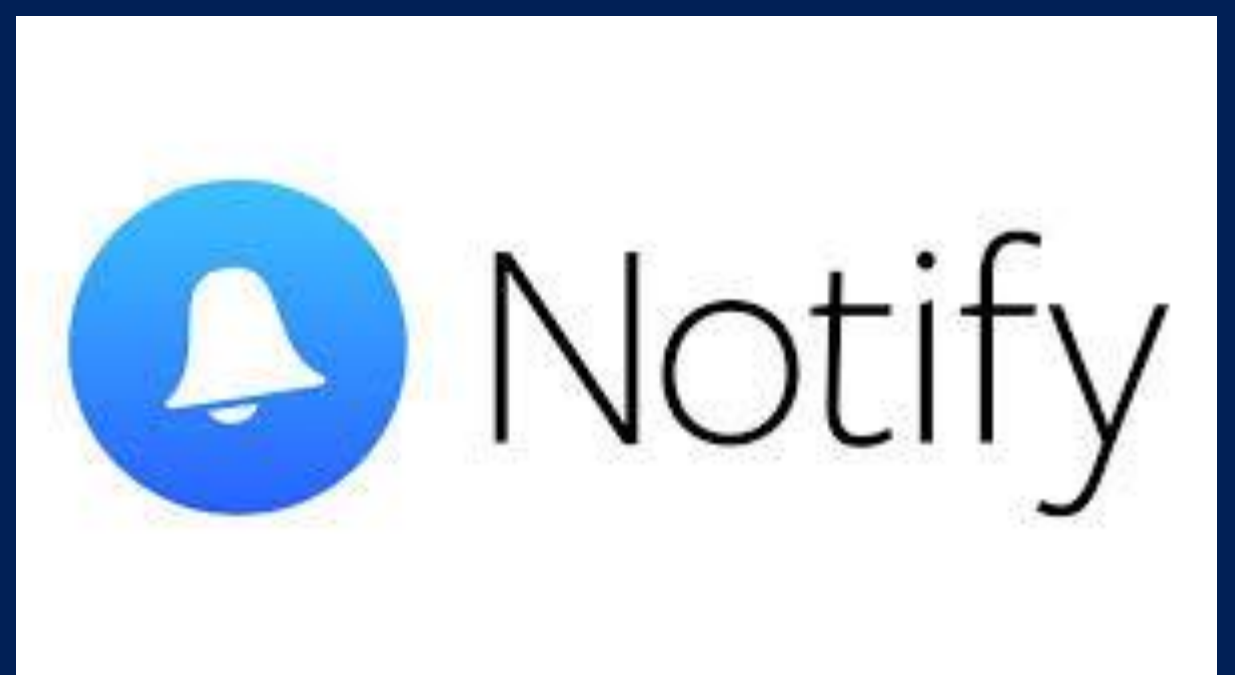
- Take a forensic image of the affected computers
- Preserve records for later analysis and use at trial
 - May require law enforcement
 - Establish a chain of custody
- Preserve logs, notes, records, and data
- Maintain records related to continuing attacks



Post-breach Execution – Incident Response Plan

Notify

- People within the organization
 - Incident response team
 - Impacted employees
- Law enforcement if suspect criminal activity
 - FBI and U.S. Secret Service
- Other potential victims
 - Corporate partners



State Data Breach Notification Laws

- Forty-eight states have data breach notification laws
- Requires written notice to governmental entities
- New York has a data breach statute



Governmental and Regulatory Enforcement

- NYS Department of Financial Services
- U.S. Securities and Exchange Commission
- Federal Trade Commission
- U.S. Department of Justice



Private Litigation

- Class Action Shareholder lawsuits
- Individual lawsuits





Thank You!