How to Determine if an Incident is a Data Breach to Meet Compliance Obligations

Alex Wall, Sr. Counsel & Global Privacy Officer

Agenda

- Challenges to Compliance
- Overview of the Regulatory Landscape
- Is it a Breach? How to Tell and Why it Matters
- Best Practices for a Strong Culture of Compliance
- Q&A

Alex Wall
CIPP/E, CIPP/US, CIPM, FIP
Twitter: @wallatlaw
Email: alex.wall@radarfirst.com

Challenges in Incident Response

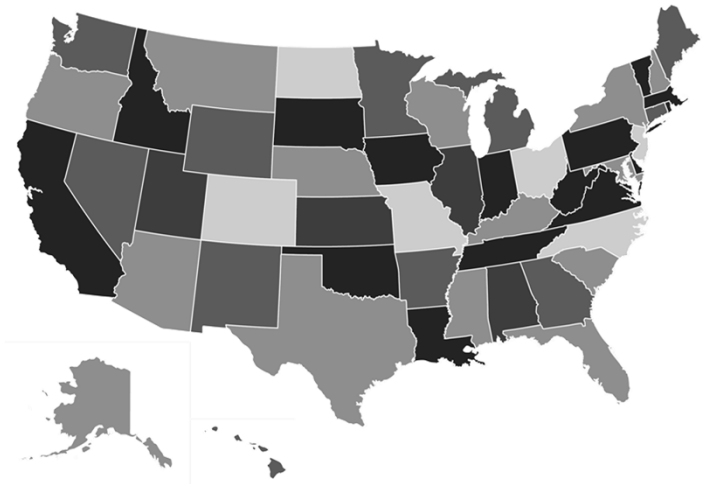
Inconsistent, risk over or under reporting

Manual, disjointed systems and incomplete documentation

Layered, complex, and ever-changing regulations

radar

Regulatory Landscape



- **2 Federal laws**, HIPAA/ HITECH and GLBA
- **48 state laws, 3 territories,** and **Washington, D.C.**
- **12+ unique agencies** you may have to report to
- **25+ proposed laws or regulations** on our regulatory watch list

radar

Event, Incident or Breach?

What's in a name? How a ***data occurrence*** is labeled will determine, among other things, who becomes involved, how the occurrence will be resolved, if notification is required, who to notify, when, and how.

radar

Event

National Institute of Standards and Technology (NIST) defines an event as "any observable occurrence in a system or network," such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection.

radar

Security Incident

An event that violates an organization's security policies and procedures. Verizon's 2016 Data Breach Investigations Report defines an incident as a "security event that compromises the integrity, confidentiality or availability of an information asset."

Privacy Incident

Defined by the Centers for Medicare & Medicaid Services (CMS), an adverse event that happened as a result of violating DHS' privacy policies and procedures, and must "pertain to the unauthorized use or disclosure" of regulated data, like personally identifiable information (PII) or protected health information (PHI).

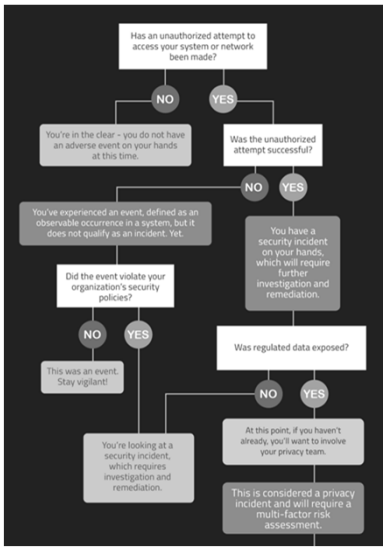
Data Breach

If a ***privacy incident*** meets specific legal definitions, per the applicable regulation or jurisdictional breach laws, then it is a ***data breach***. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies or the media.

radar

Decision Process

- Was there an unauthorized attempt to access?
- Was the attempt successful?
- Was regulated data exposed?
  - What specific data?
  - Which jurisdictions are involved?
  - Was the data recovered?
  - Was this malicious or accidental?
  - What is the risk of harm to the individual?

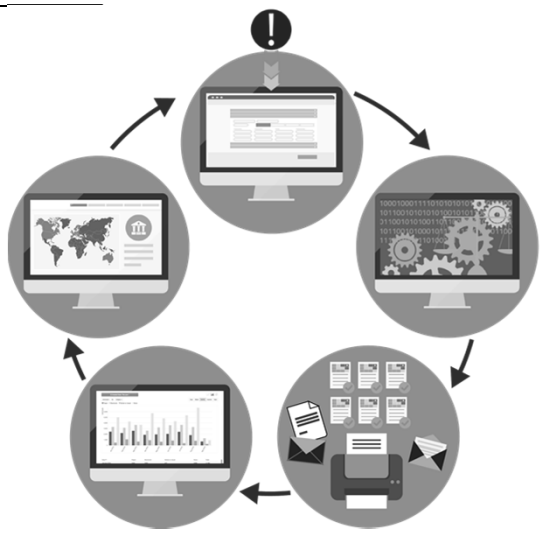


radar

Best Practices in Incident Response

Areas to operationalize incident response:

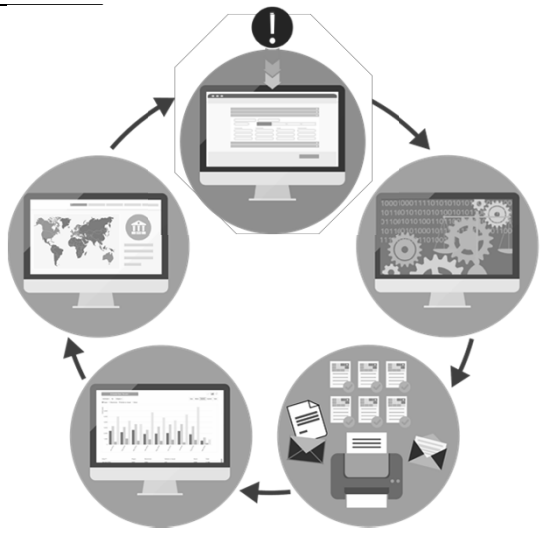
1. Incident Intake
2. Risk Assessment
3. Notification
4. Trend Analysis and Reporting
5. Stay Current with Regulations



radar

Streamline Incident Intake

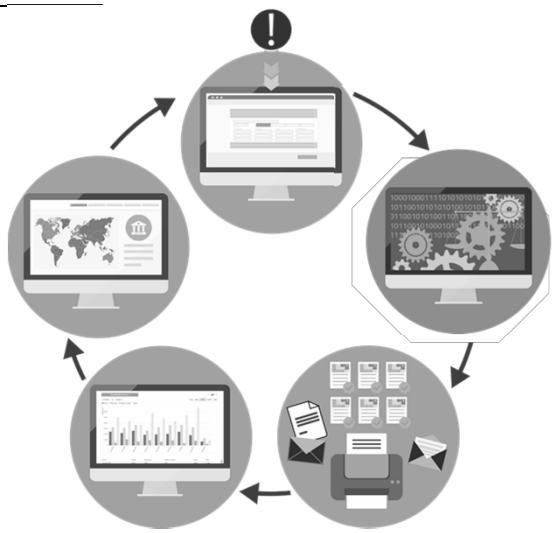
- Configurable Web Forms
- Efficient for getting the required incident details
- Automated alerts to privacy & security
- APIs for Integration
- Purpose-built Workflow



radar

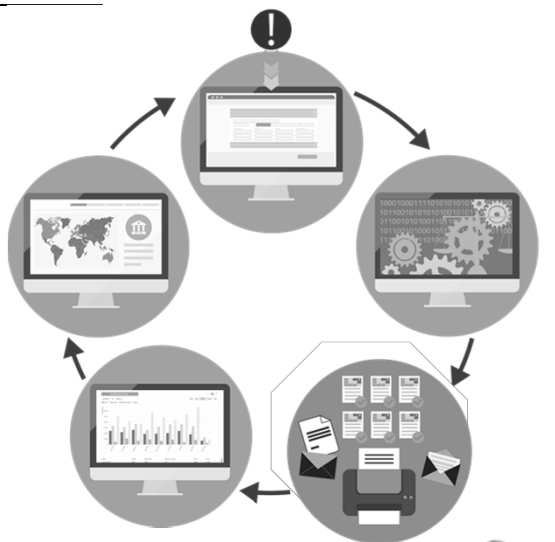
Multi-Factor Risk Assessment

- Consistent
- Efficient & Agile
- Collaborative
- Legal Oversight
- Decision-Support
- Establish Burden-of-proof



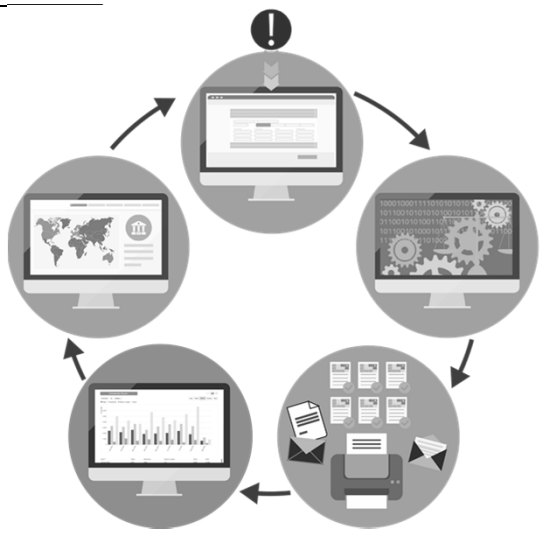
Provide Notice and Documentation

- Integrate systems that manage complete IR lifecycle
- Keep approved letter templates for individuals, agencies, clients
- Maintain a central repository of all notifications to prove compliance
- Pay special attention to deadlines, content, format – even font size



Example Consider Key Performance Indicators

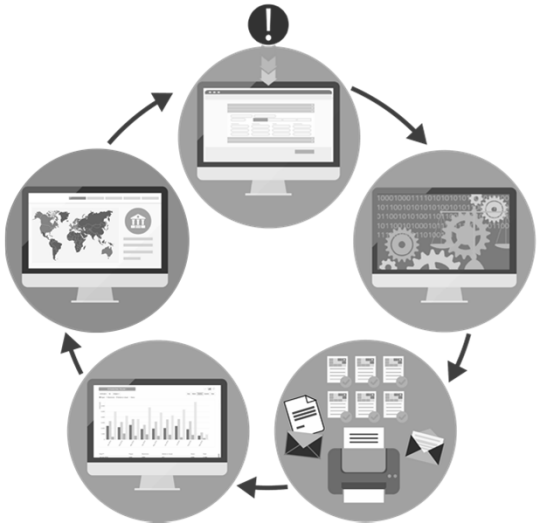
- Average time between:
  - discovery & reporting to privacy office
  - Incident creation to closure
- Percentage of incidents requiring mandatory notification, contractual notification, or involving multiple jurisdictions
- Frequency of missed notification due dates (regulatory & contractual)
- Incident volume, source, type, etc.



radar

Keep Current with Regulations

Following are three examples of the regulatory complexity we see across jurisdictions...



radar

Examples of Regulatory Complexity: 1/3

Alternate compliance in Washington

Certain exemptions to notification requirements are allowed in the state, *except* when it comes to notifying the state AG.

…which means a HIPAA-regulated entity could be exempt from providing notice under HIPAA, but would still need to provide notice to the state attorney general

radar

Examples of Regulatory Complexity: 2/3

Employer or Payroll info in Virginia

Effective July 1, 2017, the state requires notice be provided to the state attorney general if certain employee payroll data is compromised.

…which means in this state, you'll need to additionally consider if the incident includes *taxpayer identification number* in combination with the *income tax withheld for the taxpayer*.

radar

Examples of Regulatory Complexity: 3/3

Notice to HHS Triggers Attorney General Notification Requirements in Illinois

Effective July 1, 2017, the state requires notice be provided to the state attorney general if the department of Health and Human Services requires notification.

…which means HIPAA-regulated entities will need to be aware of the dependencies for notification requirements in this state.

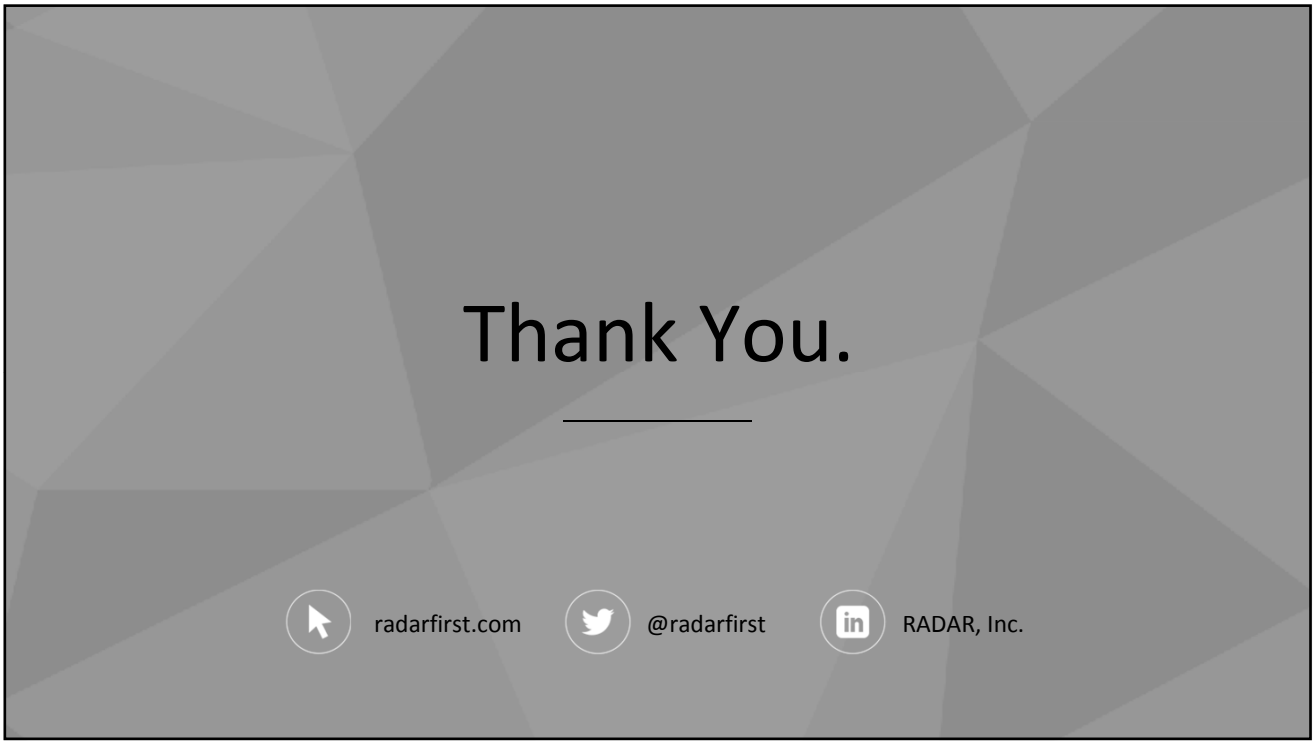
radar

Words of Encouragement

"Privacy is everybody's job, and it's bigger than a compliance issue: it's a business issue because it's about trust. If your business depends on relationships with people, then your success depends on your ability to do a good job at privacy."

radar


Questions?


Thank You.
radarfirst.com
@radarfirst
RADAR, Inc.