RadarFirst

iapp

international association of privacy professionals

To Notify or Not to Notify? That Is the Question.

Thursday, January 30, 2019
Time: 8:00–9:00 a.m. PT
11:00 a.m.–12:00 p.m. ET
5:00–6:00 p.m. CET

www.iapp.org

Welcome & Introductions

Host:

Dave Cohen
CIPP/US, CIPP/E
Knowledge Manager
IAPP

Speakers:

Mahmood Sher-Jan
CHPC
CEO & Founder
RadarFirst

Holly Amorosana
CIPP/US, JD
Chief Privacy Officer
Apple Bank

Agenda

- Things to consider before assessing an incident
- Operational phases of the incident response lifecycle
- Incident Risk Assessment Scenarios
- Elements of an effective incident response program
- Benchmarking highlights
- Q&A

Incident response lifecycle

Identify & Investigate

- Incident is detected by infosec or reported by an internal or external source.
- Clock is ticking for the IR team to investigate, involve key stakeholders, and capture the info needed to drive a risk assessment.

Risk Assess & Decide

- Using info gathered, IR team must accurately determine whether notification to regulators and/or individuals is required based on all applicable regulations in different nations and states.

Breach Notification

- If notification is required, IR team must notify regulators and individuals of the breach in time to meet all regulatory deadlines.
- Notification must contain the info required in each jurisdiction, and delivery must be tracked and documented.

Reporting & Trend Analysis

- Incident is detected by infosec or reported by an internal or external source.

Risk Assess & Decide: Things to consider ahead of time

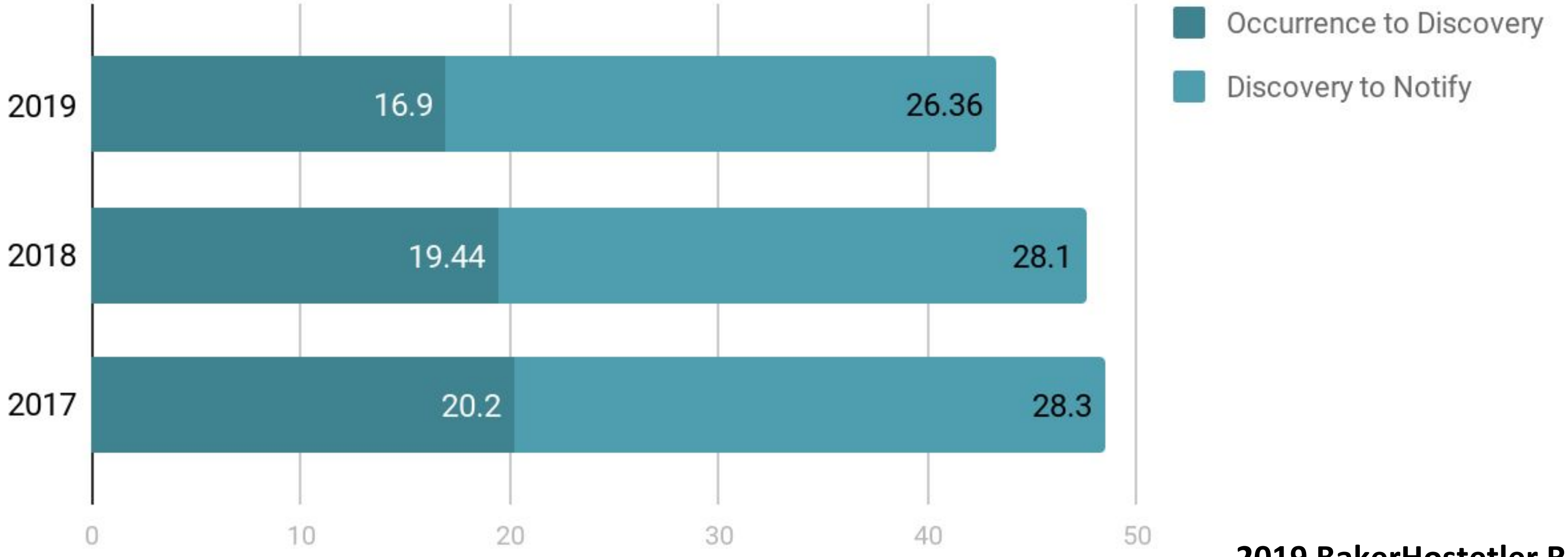
- Who is **responsible** for the incident risk assessment and notification decision?
- Defined and documented incident assessment process including ensuring consistency, objectivity and defensibility
- What processes and tools are used by the team to operationalize the incident assessment and decision making process
- How does the response team communicate and make final decisions

Effective Risk Assessment is Essential for Organizational Risk Mitigation

A mature multi-factor risk assessment is the foundation for effective and timely decision-making and ensuring compliance in a complex and changing regulatory landscape.

Consistent	Objective	Timely	Defensible
Same incident scenario but varying and inconsistent notification decisions create risk and draw attention to a program that is ad-hoc & lacking the necessary maturity.	Notification decision should be objective based on documented multi-factor risk assessment that is compliant with applicable regulations.	Your team needs to arrive at the right notification decision in time to meet compliance deadlines for all applicable regulation.	Demonstration of consistency and objectivity of the incident risk assessment and notification decisions are key to establishing defensibility.

Incident lifecycle time periods

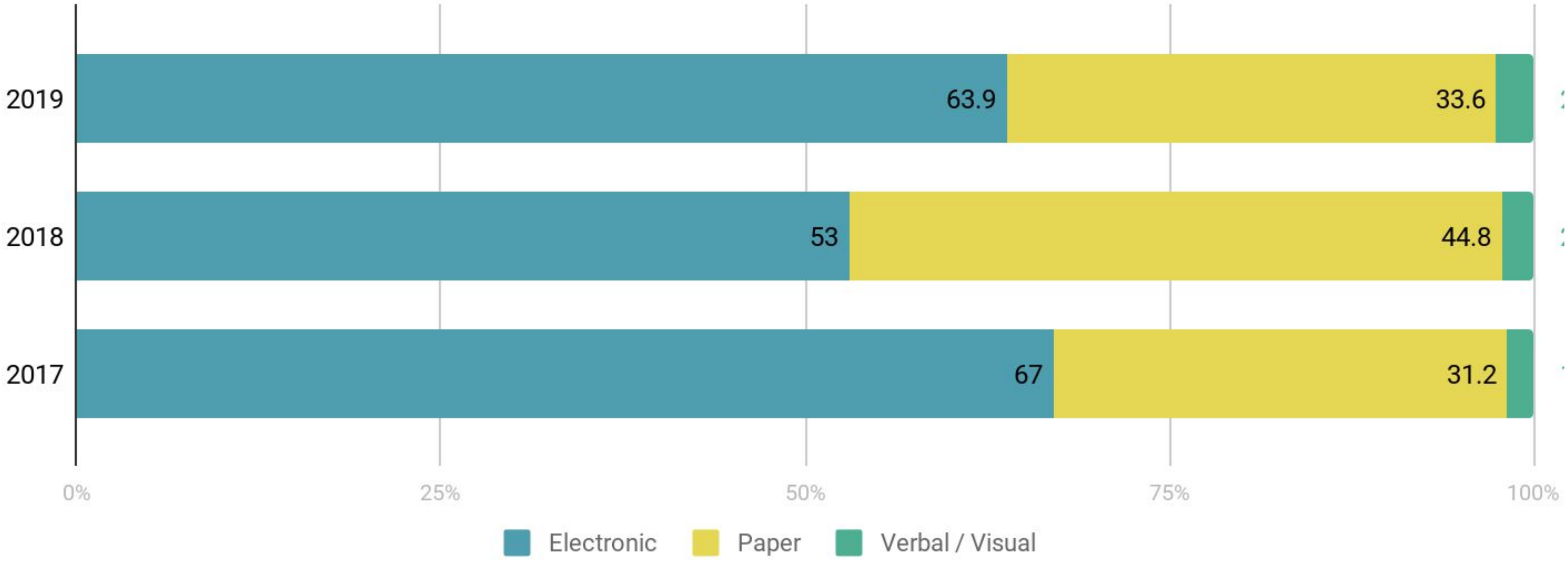


2019 BakerHostetler Report:

Occurrence to discovery = 66 days

Discovery to notify = 56 days

Electronic vs. Paper vs. Verbal/Visual



Let’s dive into scenarios!

Scenario #1- Identify & Investigate

You've just been informed an employee from an internal business unit mistakenly emailed a file containing customer data to an incorrect person outside the organization.

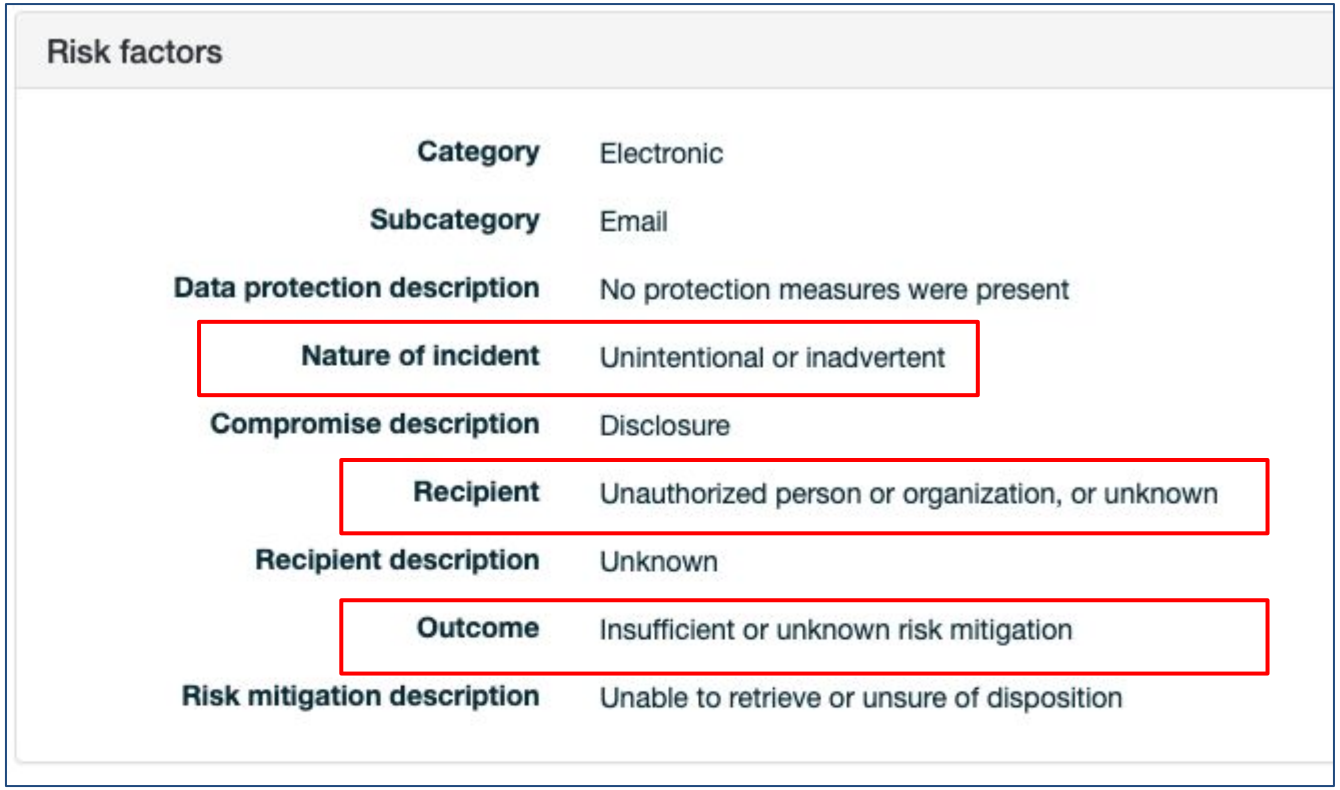
The employee was attempting to email the file to a coworker, however made a typo on the email address and ended up sending the file of customer data to some unknown person.

Scenario #1 - Identify & Investigate

Data Elements Exposed:

- Names
- Mailing address including city, state and zip
- Phone Numbers
- Email address (which also functions as the online username for account access)

Scenario #1 - Risk Assessment



Risk factors

Category	Electronic
Subcategory	Email
Data protection description	No protection measures were present
Nature of incident	Unintentional or inadvertent
Compromise description	Disclosure
Recipient	Unauthorized person or organization, or unknown
Recipient description	Unknown
Outcome	Insufficient or unknown risk mitigation
Risk mitigation description	Unable to retrieve or unsure of disposition

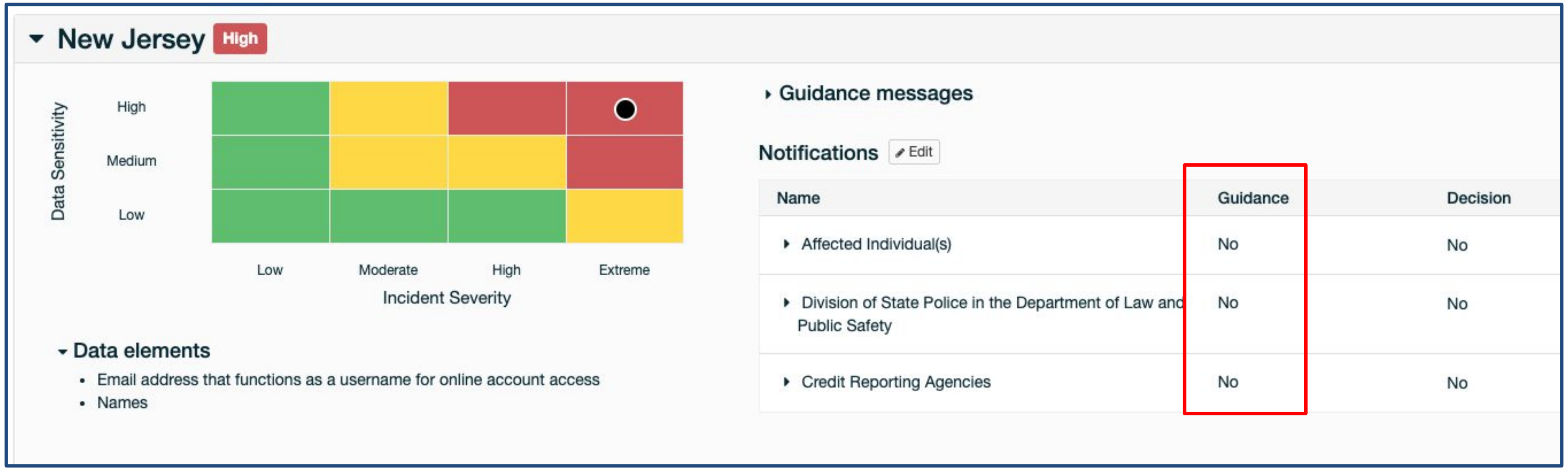
- **Risk Factors:**
  - Recipient of the data
    - Were they authorized, not authorized, generally authorized?
  - Nature of the incident
  - Data protection measures
  - Risk mitigation measures

Email mistakenly sent to a random person outside the organization who is not authorized to see the data.

Scenario #1 - Notification Decision

Would your organization notify the impacted individuals?

Scenario #1 - Your Decision



New Jersey High

Data Sensitivity

	Low	Moderate	High	Extreme
High	🟩	🟨	🟥	🟥 ●
Medium	🟩	🟨	🟨	🟥
Low	🟩	🟩	🟩	🟨

Incident Severity

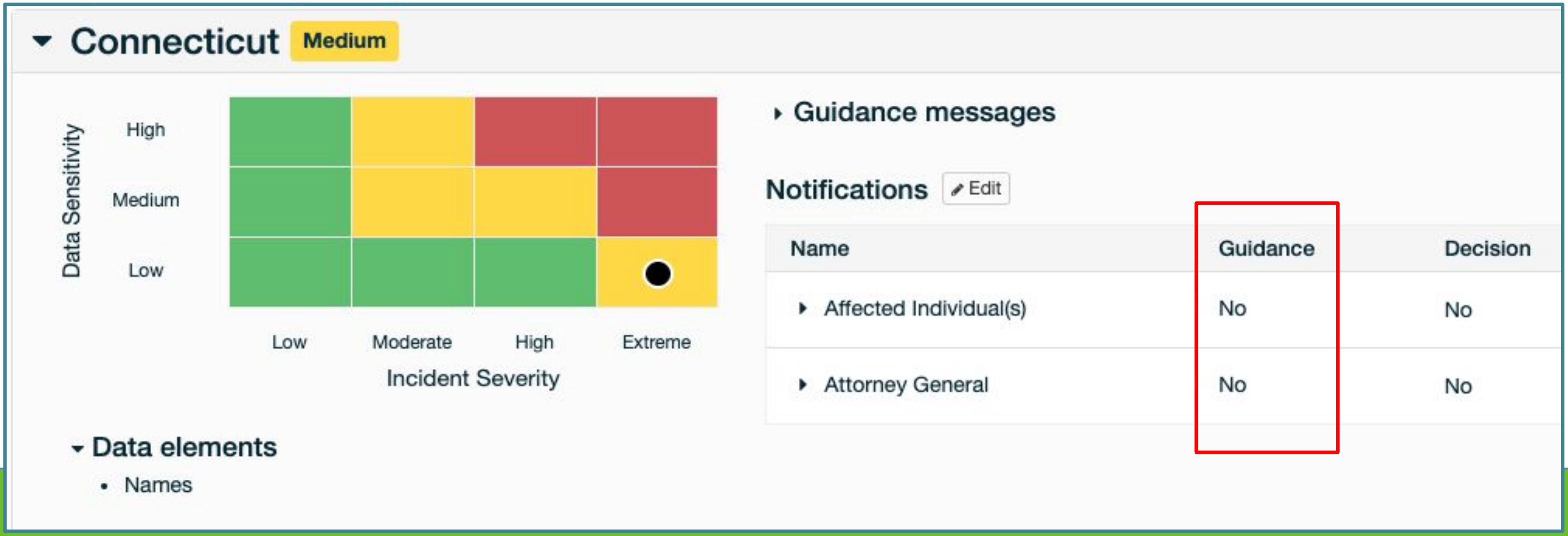
Data elements

- Email address that functions as a username for online account access
- Names

Guidance messages

Notifications Edit

Name	Guidance	Decision
Affected Individual(s)	No	No
Division of State Police in the Department of Law and Public Safety	No	No
Credit Reporting Agencies	No	No



Connecticut Medium

Data Sensitivity

	Low	Moderate	High	Extreme
High	🟩	🟨	🟥	🟥
Medium	🟩	🟨	🟨	🟥
Low	🟩	🟩	🟩	🟨 ●

Incident Severity

Data elements

- Names

Guidance messages

Notifications Edit

Name	Guidance	Decision
Affected Individual(s)	No	No
Attorney General	No	No

Guidance Message:
Does not meet New Jersey or Connecticut’s definition of sensitive customer or personal information. **Notification is not expected in either state under the law.**

Scenario #1 - But, What If…

What if you looked at the file again and noticed passwords were also included in the emailed file, it was just in a hidden field?

Scenario #1 - Identify & Investigate

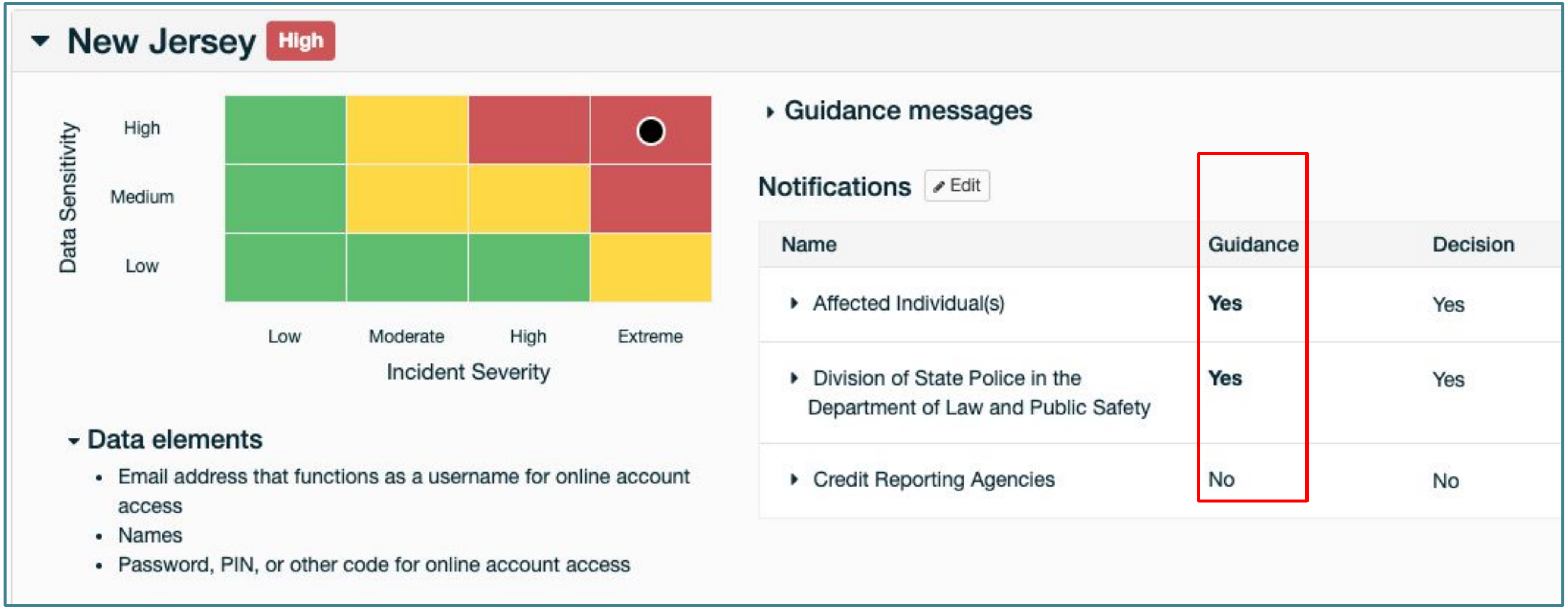
Data Elements Exposed:

- Names
- Mailing address including city, state and zip
- Phone Numbers
- Email address (which functions as the online username for account access)
- Password, PIN, or other code for online account access

Scenario #1 - Decide

Does your notification decision change based on the newly discovered info?

Scenario #1 - Decide



New Jersey High

Data Sensitivity / Incident Severity

Data Sensitivity	Low	Moderate	High	Extreme
High	🟩	🟨	🟥	🟥 ●
Medium	🟩	🟨	🟨	🟥
Low	🟩	🟩	🟩	🟨

Guidance messages

Notifications Edit

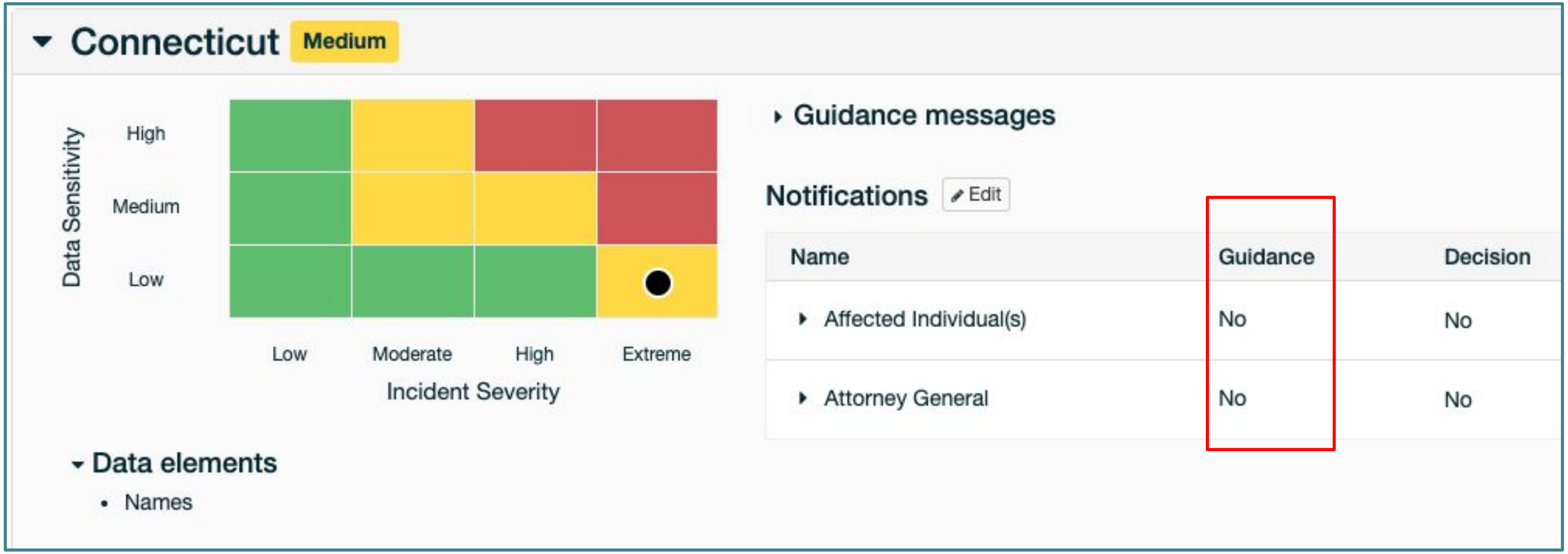
Name	Guidance	Decision
Affected Individual(s)	**Yes**	Yes
Division of State Police in the Department of Law and Public Safety	**Yes**	Yes
Credit Reporting Agencies	No	No

Data elements

- Email address that functions as a username for online account access
- Names
- Password, PIN, or other code for online account access

Notification is required in the state of New Jersey due to the inclusion of email address (that can be used as username) and password data elements, which are defined as personal information.

Scenario #1 - Decide



Connecticut Medium

Data Sensitivity	Low	Moderate	High	Extreme
High	🟩	🟨	🟥	🟥
Medium	🟩	🟨	🟨	🟥
Low	🟩	🟩	🟩	🟨 ●

Incident Severity

- Data elements
  - Names

Guidance messages

Notifications ✎ Edit

Name	Guidance	Decision
Affected Individual(s)	No	No
Attorney General	No	No

Data elements still do not meet Connecticut's definition of sensitive customer or personal information. Notification is not expected.

Scenario #2- Identify & Investigate

At an organization in Netherlands, a file containing names along with national id numbers was accidentally shared with an unauthorized processor.

We assume we'll receive sufficient mitigation since they are a processor with regulatory obligation to protect personal data, however we have requested but not gotten a written assurance from the processor yet.

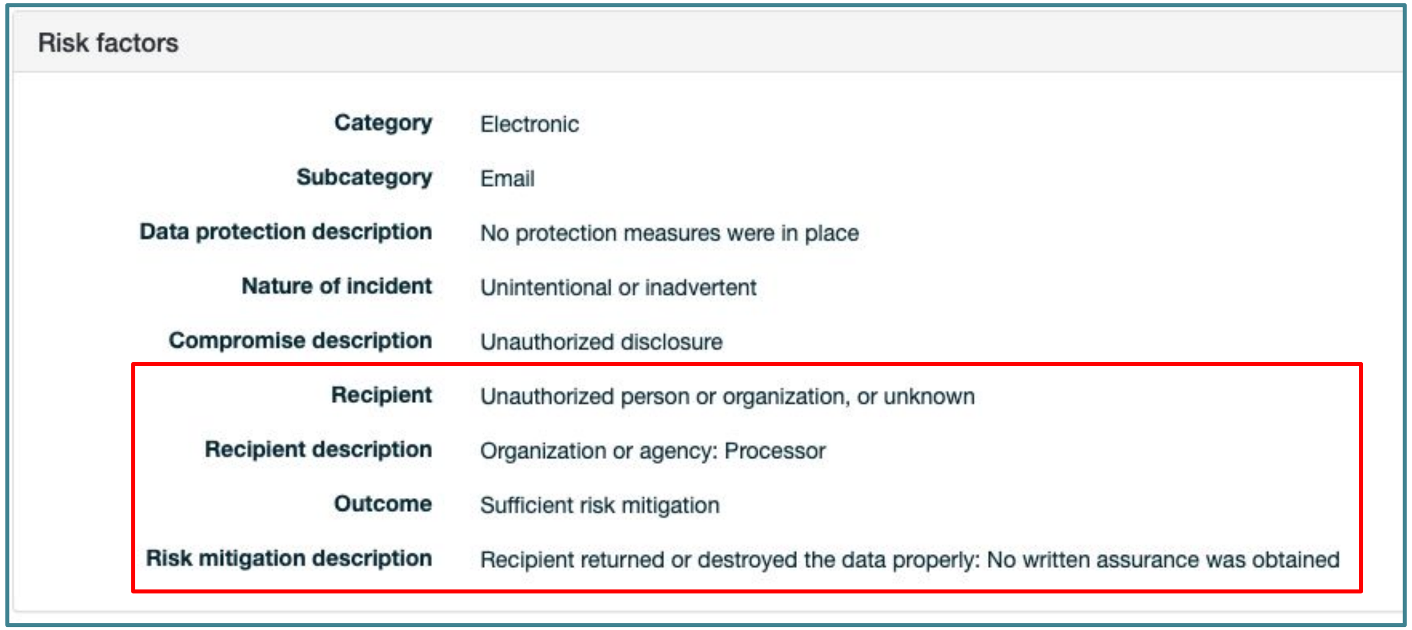
Scenario #2 - Identify & Investigate

Data Elements Exposed:

- Names
- National ID Number

Scenario #2 - Risk Assess

Region: European Union



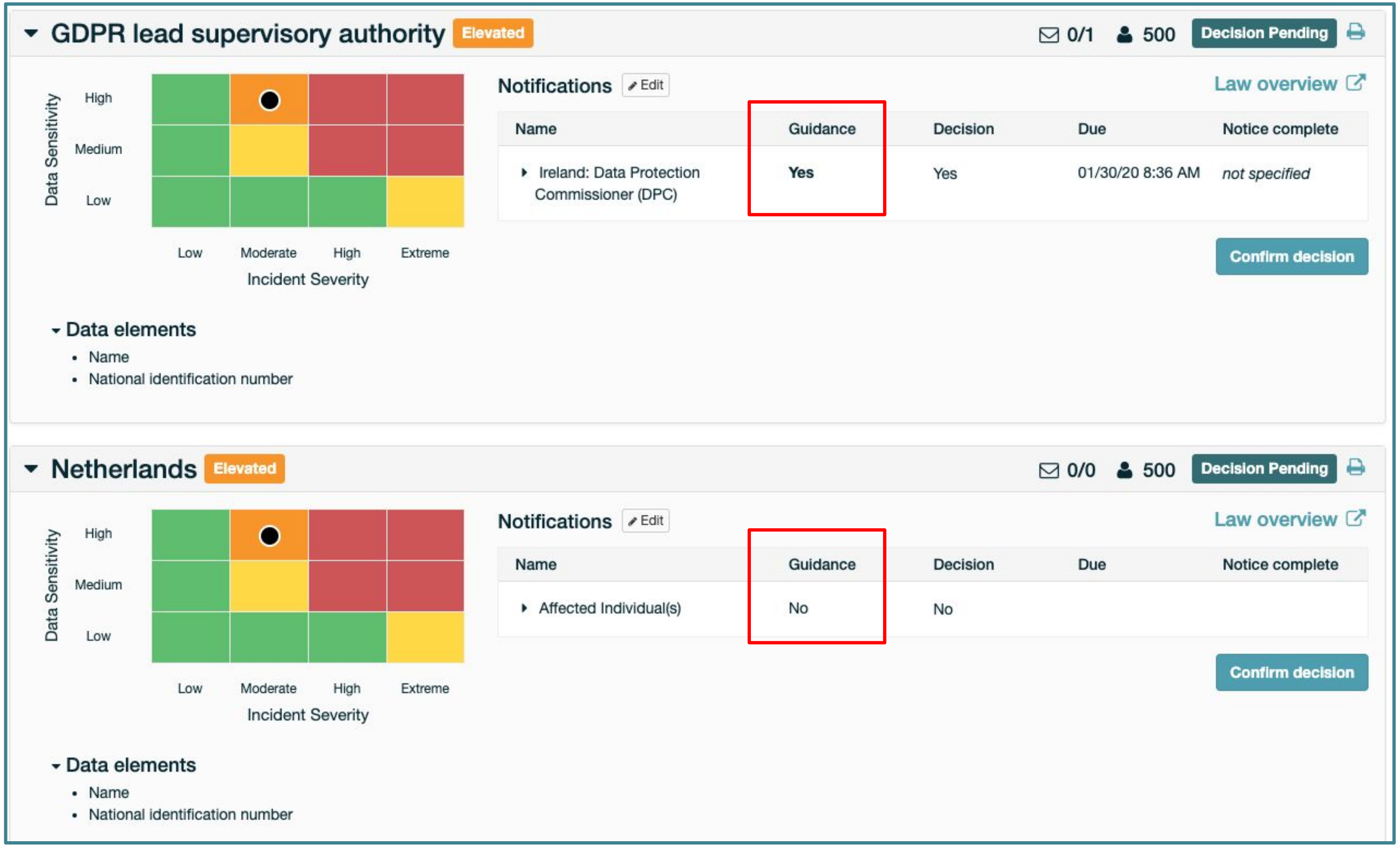
Risk factors

Category	Electronic
Subcategory	Email
Data protection description	No protection measures were in place
Nature of incident	Unintentional or inadvertent
Compromise description	Unauthorized disclosure
Recipient	Unauthorized person or organization, or unknown
Recipient description	Organization or agency: Processor
Outcome	Sufficient risk mitigation
Risk mitigation description	Recipient returned or destroyed the data properly: No written assurance was obtained

Scenario #2 - Decide

Would your organization notify the impacted individuals?

Scenario #2 - Decide



GDPR lead supervisory authority Elevated — 0/1 — 500 — Decision Pending

Notifications ✎ Edit — Law overview

Name	Guidance	Decision	Due	Notice complete
▸ Ireland: Data Protection Commissioner (DPC)	**Yes**	Yes	01/30/20 8:36 AM	*not specified*

Confirm decision

Data elements

- Name
- National identification number

Netherlands Elevated — 0/0 — 500 — Decision Pending

Notifications ✎ Edit — Law overview

Name	Guidance	Decision	Due	Notice complete
▸ Affected Individual(s)	No	No		

Confirm decision

Data elements

- Name
- National identification number

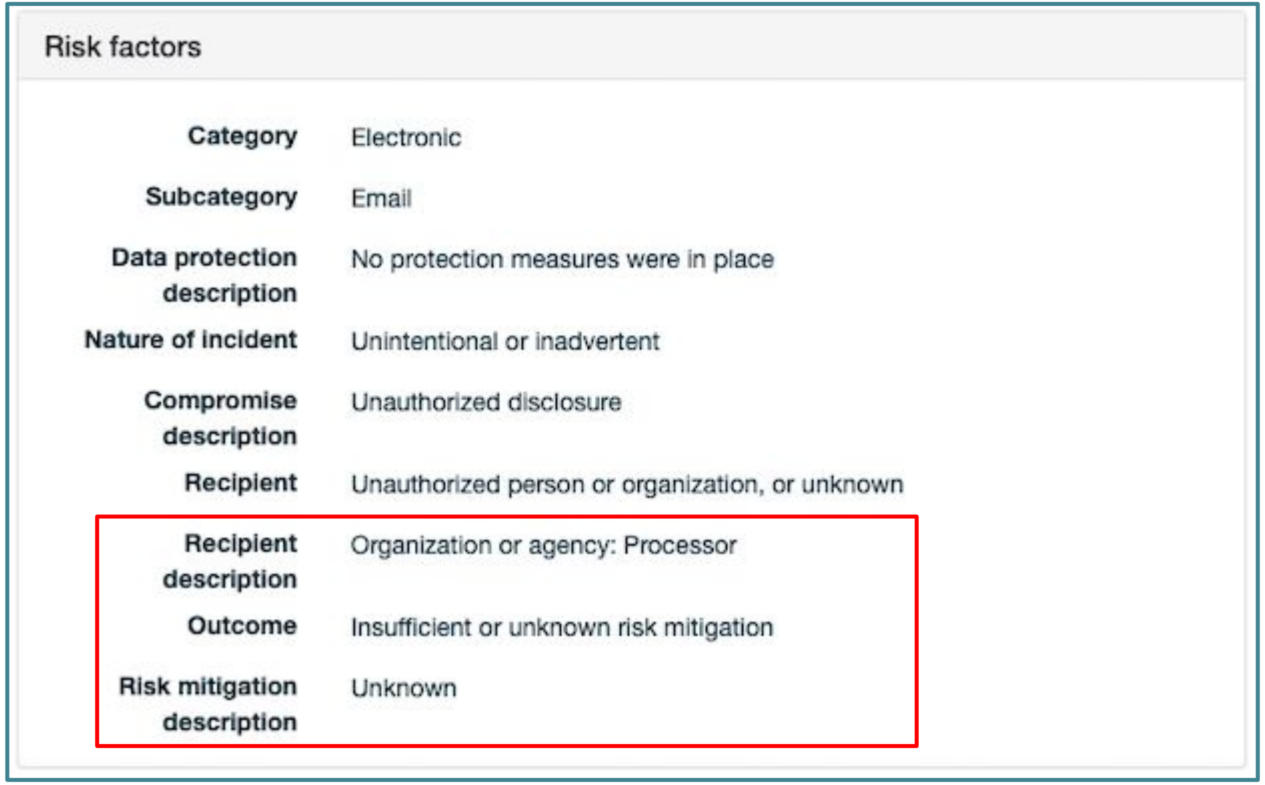
Notification required to Ireland Data Protection Commissioner, but **not required** to affected individuals.

Scenario #2 - But, What If…

As the investigation continued the processor is being non-responsive and we no longer believe we’ll be able to confirm sufficient risk mitigation.

Scenario #2 - Risk Assessment

Region: European Union



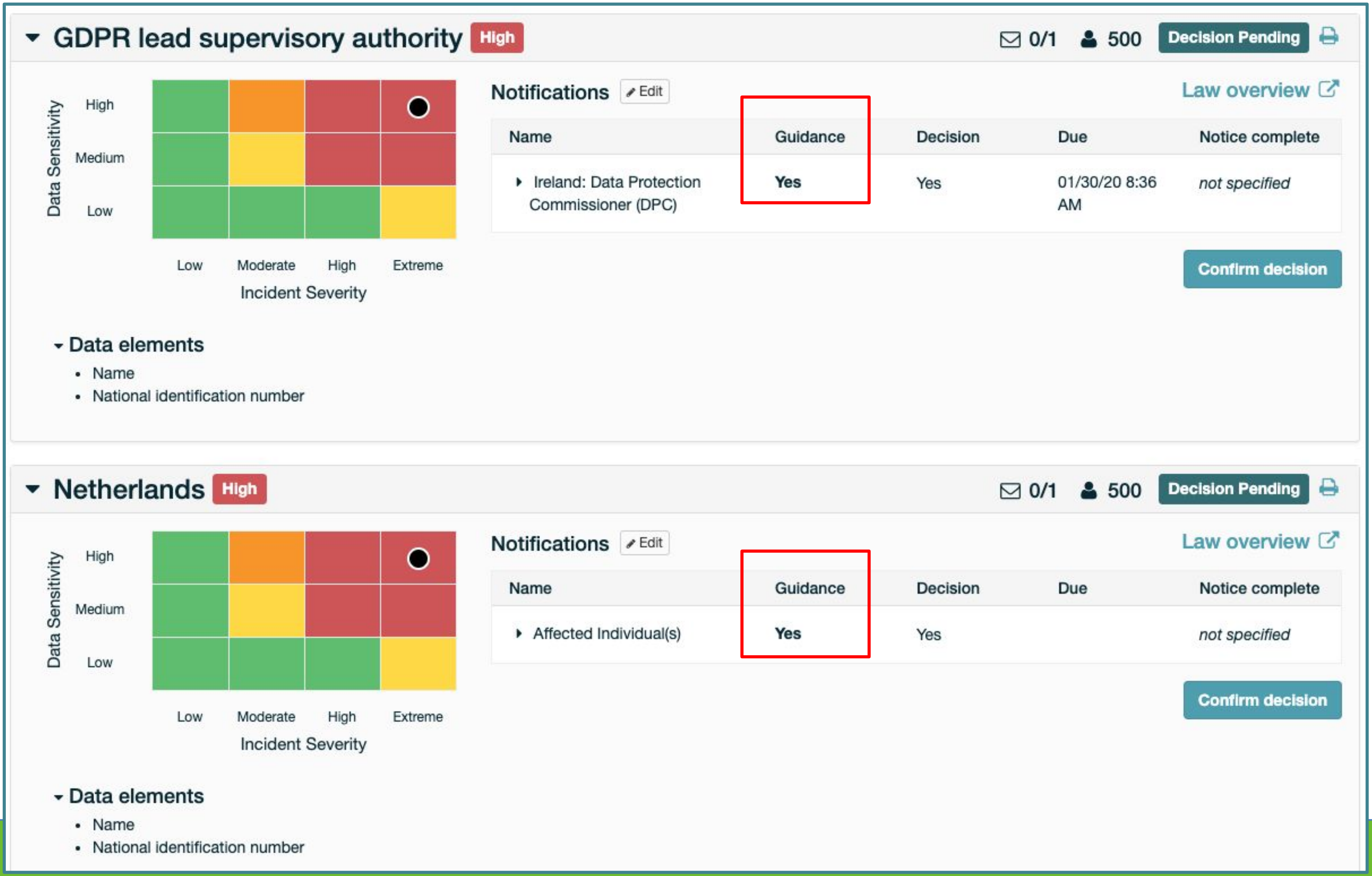
Risk factors

Category	Electronic
Subcategory	Email
Data protection description	No protection measures were in place
Nature of incident	Unintentional or inadvertent
Compromise description	Unauthorized disclosure
Recipient	Unauthorized person or organization, or unknown
Recipient description	Organization or agency: Processor
Outcome	Insufficient or unknown risk mitigation
Risk mitigation description	Unknown

Scenario #2 - Decide

Does your notification decision change based on the revised info?

Scenario #2 - Risk Assess



GDPR lead supervisory authority High

0/1 · 500 · Decision Pending

Data Sensitivity

	Low	Moderate	High	Extreme
High	🟩	🟧	🟥	🟥 ●
Medium	🟩	🟨	🟥	🟥
Low	🟩	🟩	🟩	🟨

Incident Severity

Notifications Edit

Law overview

Name	Guidance	Decision	Due	Notice complete
Ireland: Data Protection Commissioner (DPC)	**Yes**	Yes	01/30/20 8:36 AM	*not specified*

Confirm decision

Data elements

- Name
- National identification number

Netherlands High

0/1 · 500 · Decision Pending

Data Sensitivity

	Low	Moderate	High	Extreme
High	🟩	🟧	🟥	🟥 ●
Medium	🟩	🟨	🟥	🟥
Low	🟩	🟩	🟩	🟨

Incident Severity

Notifications Edit

Law overview

Name	Guidance	Decision	Due	Notice complete
Affected Individual(s)	**Yes**	Yes		*not specified*

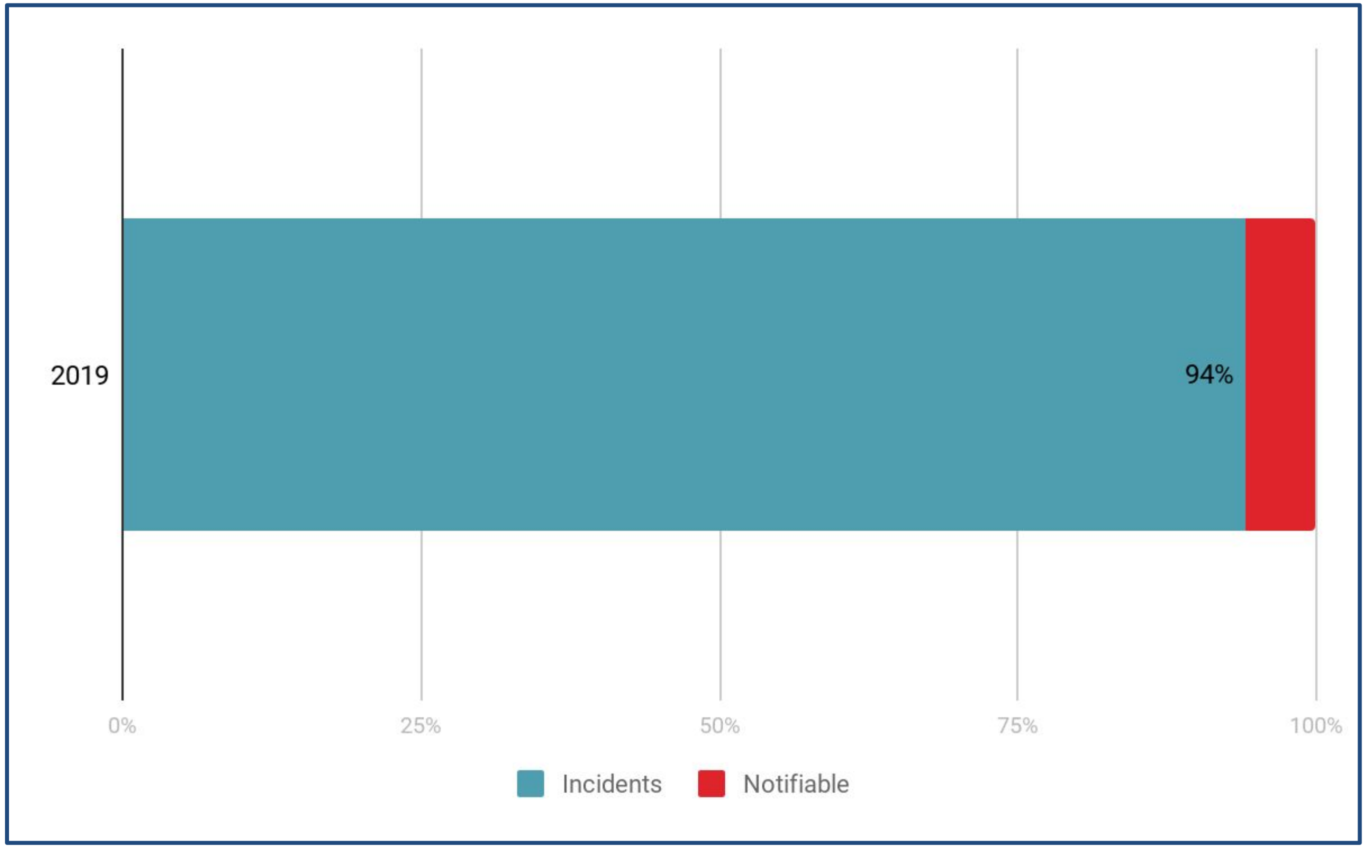
Confirm decision

Data elements

- Name
- National identification number

Notification required to **both** Data Protection Commissioner and affected individuals.

What is an optimal notification rate?



- Sufficient risk mitigation is crucial in reducing risk of harm.
- Consistent and objective multi-factor risk assessment provides the necessary proof of compliance.

Risks of over or under - reporting

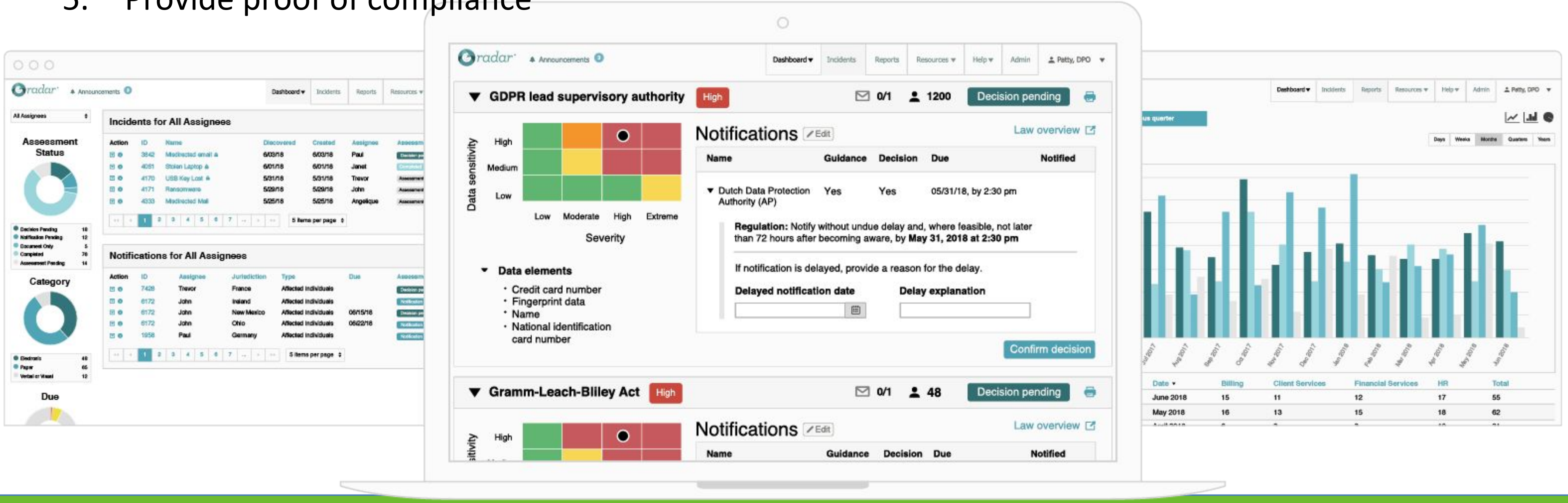
- **Risks of over-reporting**
  - Brand and reputational damage
  - Erosion of confidence from your customers
  - Greater regulatory scrutiny from authorities and auditors
  - Increased operational costs

- **Risks of under-reporting:**
  - Fines and penalties
  - Diminishing consumer confidence which in turn impacts bottom line
  - M&A implications

Simplify compliance with automation

RADAR provides **consistency** and **efficiency** by operationalizing incident response:

1. Simplify incident escalation & details
2. Quickly assess whether an incident requires notification to supervisory authority and data subjects
3. Manage third party data processing notification obligations
4. Monitor trends and measure program metrics
5. Provide proof of compliance



● Decision Pending	18
● Notification Pending	12
● Document Only	5
● Completed	76
● Assessment Pending	14

● Electronic	48
● Paper	65
● Verbal or Visual	12

Incidents for All Assignees

Action	ID	Name	Discovered	Created	Assignee	Assessm
	3842	Misdirected email	6/03/18	6/03/18	Paul	Decision p
	4061	Stolen Laptop	6/01/18	6/01/18	Janet	Completed
	4170	USB Key Lost	5/31/18	5/31/18	Trevor	Assessment
	4171	Ransomware	5/29/18	5/29/18	John	Assessment
	4333	Misdirected Mail	5/25/18	5/25/18	Angelique	Assessment

Notifications for All Assignees

Action	ID	Assignee	Jurisdiction	Type	Due	Assessm
	7428	Trevor	France	Affected individuals		Decision p
	6172	John	Ireland	Affected individuals		Notification
	6172	John	New Mexico	Affected individuals	06/15/18	Decision p
	6172	John	Ohio	Affected individuals	06/22/18	Notification
	1958	Paul	Germany	Affected individuals		Notification

▼ GDPR lead supervisory authority High 0/1 1200 Decision pending

Notifications

Name	Guidance	Decision	Due	Notified
▼ Dutch Data Protection Authority (AP)	Yes	Yes	05/31/18, by 2:30 pm	

Regulation: Notify without undue delay and, where feasible, not later than 72 hours after becoming aware, by **May 31, 2018 at 2:30 pm**

If notification is delayed, provide a reason for the delay.

Delayed notification date

Delay explanation

▼ **Data elements**

- Credit card number
- Fingerprint data
- Name
- National identification card number

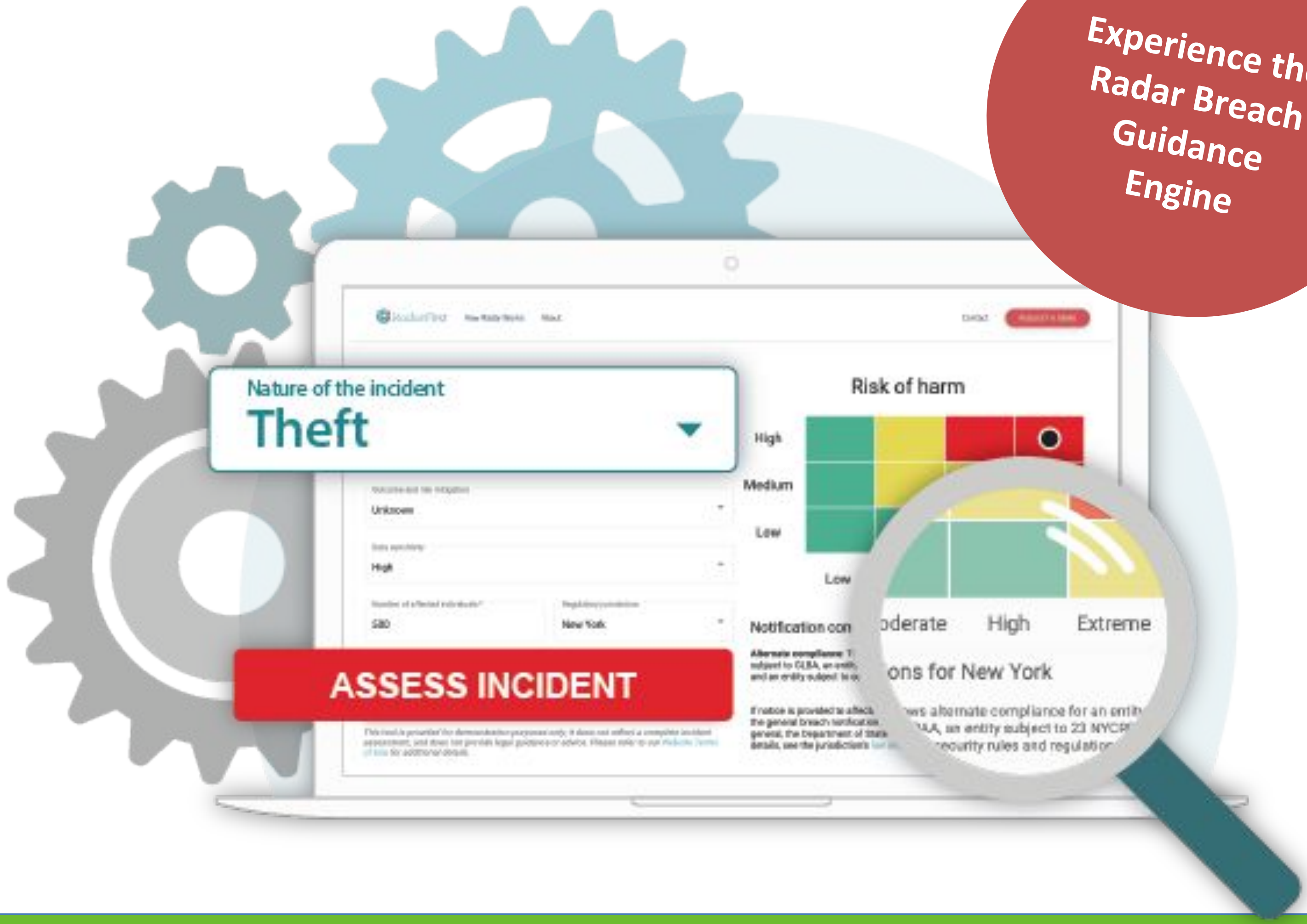
▼ Gramm-Leach-Bliley Act High 0/1 48 Decision pending

Notifications

Name	Guidance	Decision	Due	Notified

Date ▾	Billing	Client Services	Financial Services	HR	Total
June 2018	15	11	12	17	55
May 2018	16	13	15	18	62

Is it a breach? Automation in Incident Response

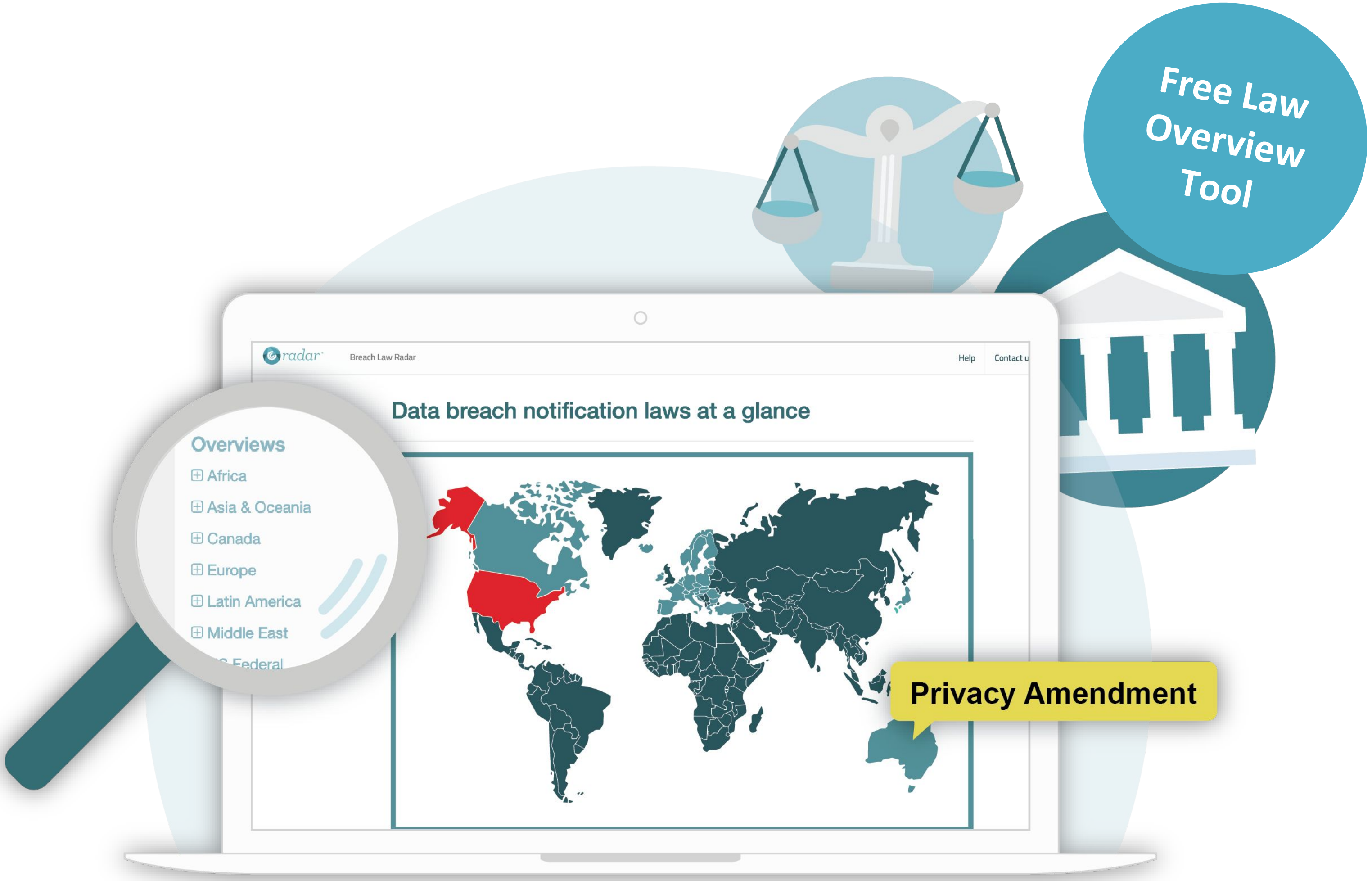


Experience the Radar Breach Guidance Engine

See firsthand how the Radar Breach Guidance Engine cuts incident response efforts in half - ensuring consistent, objective results

https://breach-engine.radarfirst.com/

Stay Current with Changing Breach Laws



Data breach notification laws at a glance

Overviews
- ⊞ Africa
- ⊞ Asia & Oceania
- ⊞ Canada
- ⊞ Europe
- ⊞ Latin America
- ⊞ Middle East
- ⊞ US Federal

Enables organizations to:
Access up-to-date overviews of global breach notification laws (including CCPA and GDPR)

Remain informed of US federal and state incident risk assessment and reporting requirements for data breaches

Keep up with the requirements to achieve regulatory compliance and the penalties for non-compliance

radarfirst.com/breach-law

Questions & Answers

Host:

Dave Cohen
CIPP/US, CIPP/E
Knowledge Manager
IAPP

Speakers:

Mahmood Sher-Jan
CHPC
CEO & Founder
RADAR

Holly Amorosana
CIPP/US, JD
Chief Privacy Officer
Apple Bank

THANK YOU!

To our speakers, our sponsor, and to all of you in the virtual audience.

RadarFirst

Marketing Preferences

This web conference is being provided to you free of charge thanks to the generous support of our sponsor. In exchange for this support, we provide the sponsor with registrant contact information under strict guidelines. If you would like to opt-out of being contacted by our sponsor, you may express your preferences here: Radarfirst's privacy policy.

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://www.questionpro.com/t/AOhP6ZgIgP

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/G, CIPP/C, CIPT or CIPM credential worth 1.0 credit hours. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: CPE credit application.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body’s rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings or to obtain a copy of the slide presentation please contact:

Dave Cohen, CIPP/E, CIPP/US
Knowledge Manager
International Association of Privacy Professionals (IAPP)
dave@iapp.org
603.427.9221