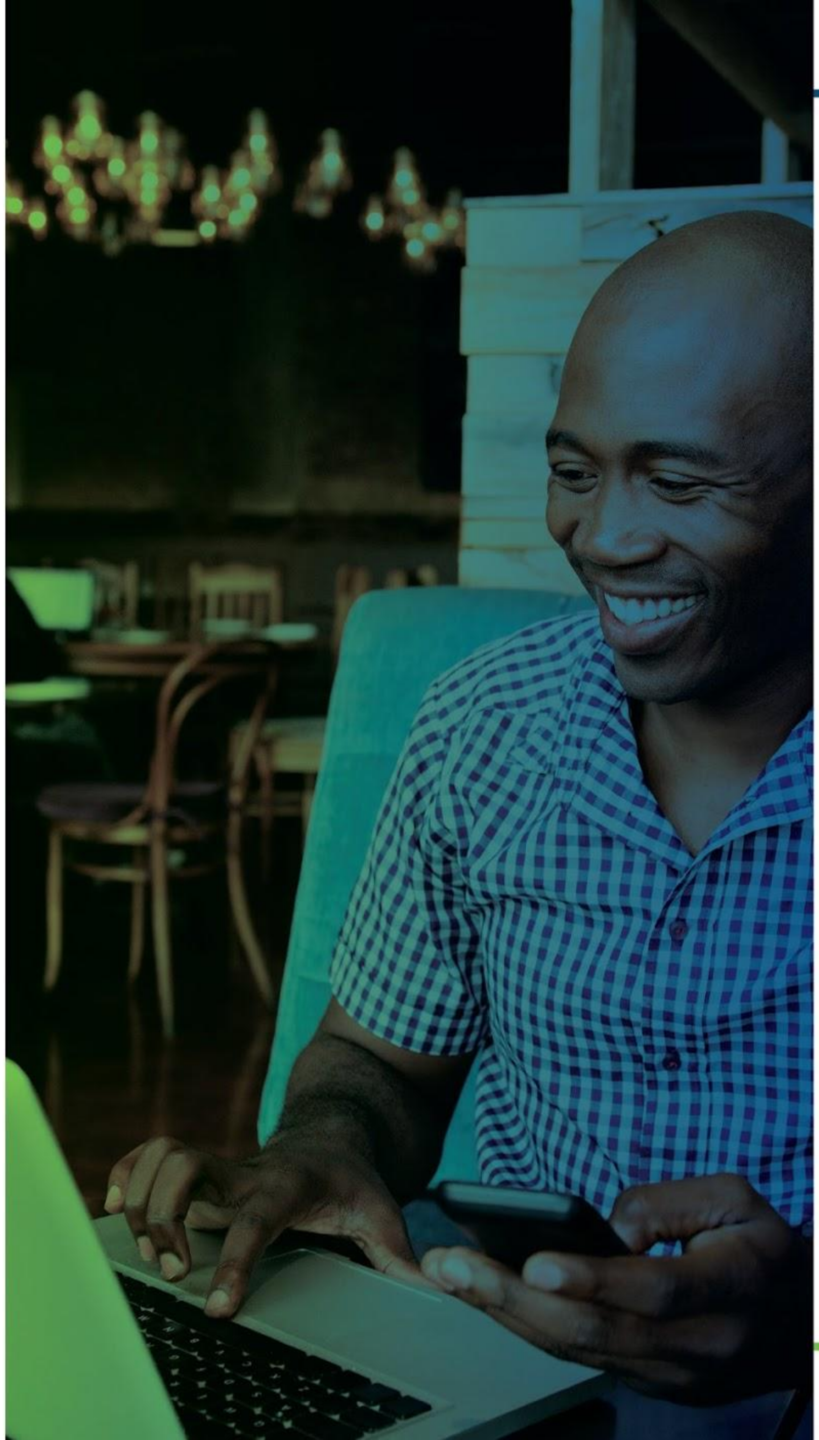


iapp

RadarFirst

The Privacy Incident Benchmark Report: Data to Drive Operational Excellence

Wednesday, March 25th, 2020

Time: 8:00–9:00 a.m. PT
11:00 a.m.–noon ET
5:00–6:00 p.m. CET

Welcome & Introductions

Host:

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

Speakers:

Mahmood Sher-Jan
CHPC
CEO & Founder
RadarFirst

Michelle Wraight
CISM, CRISC
Director & Global Head of Privacy Automation
BNY Mellon

Today’s Agenda

- Welcome & Introductions
- Why benchmarking matters
- Analyzing your incident response data: KPIs and metrics to monitor
- Benchmarking your privacy program through incident response data
- Actionable insights: turning your analysis into practical use
- Tools & recommendations
- Questions & Answers

The incident response lifecycle

Identify & Investigate

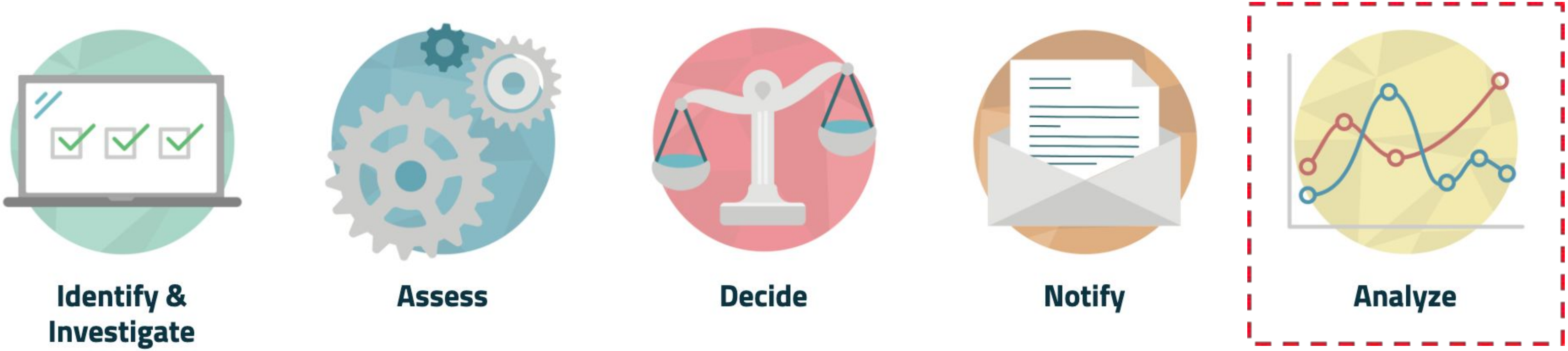
Assess

Decide

Notify

Analyze

The incident response lifecycle



Identify & Investigate

Assess

Decide

Notify

Analyze

“Price of light is less than the cost of darkness.”

- Arthur Nielsen

Why tracking metrics matters

- Draws a line in the sand for your incident response program
- Helpful in determining the health of your program in comparison to your peers
- To better understand what areas to focus improvement efforts on
- To evaluate performance & share across departments, executives, and board members
- To prove ROI and secure/justify budget/investment

Primary drivers & audience

Drivers:

- Justification of incident response program budget & ROI
- Data driven business decisions (resources & systems)
- Elevate visibility of the incident response program within the organization
- Measure the health of your IR program for continued improvement and training

Audience:

- Quarterly or periodic audits and reports for regulators
- Board /executive level members
- Internal incident response program management team
- Risk management or other business units within the organization

Key metrics to monitor

- Volume of incidents
- Per month, per quarter, per year - look for seasonal trends
- Volume of notifiable breaches
- Distribution of large vs. small breaches
- Number of individuals impacted per incident & per breach
- Root cause
- Line of business or functional area (HR, Accounting, Customer Success)
- Incidents by client
- Distribution of paper vs. electronic vs verbal/visual vs biometric incidents
- Internal vs. external
- Malicious vs. non-malicious
- Incidents caused by third parties such as vendors or business associates
- Required vs voluntary notification
- Internal escalation timeline (occurrence > discovery & discovery > notify)
- By level of severity or degree of risk

Incident Response Benchmarking Metrics

Useful questions to ask yourself

- Do we suffer from more malicious incidents than others in our industry?
- Are we seeming to notify much more often than others?
- Are we taking much longer to notify than most?
- Are we slow to identify and escalate incidents?
- Do we have more incidents coming from external sources in comparison to others in our industry?
- Are we having more incidents of a certain type than others? (ie. more paper incidents than others in our industry)

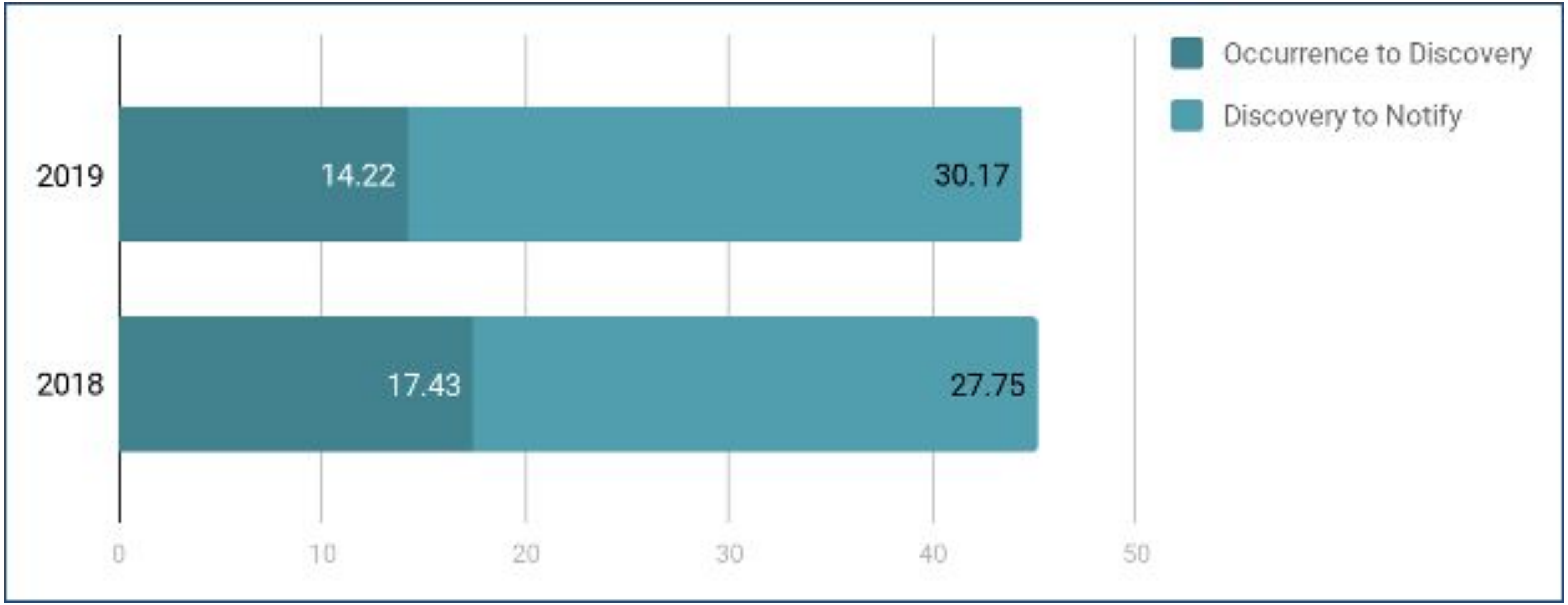
About the data

- Date range for following data: 2018 and 2019
- All incident data has been aggregated and anonymized
- Primary industries represented include financial services, healthcare, and insurance
- Largely US-centric

Definitions

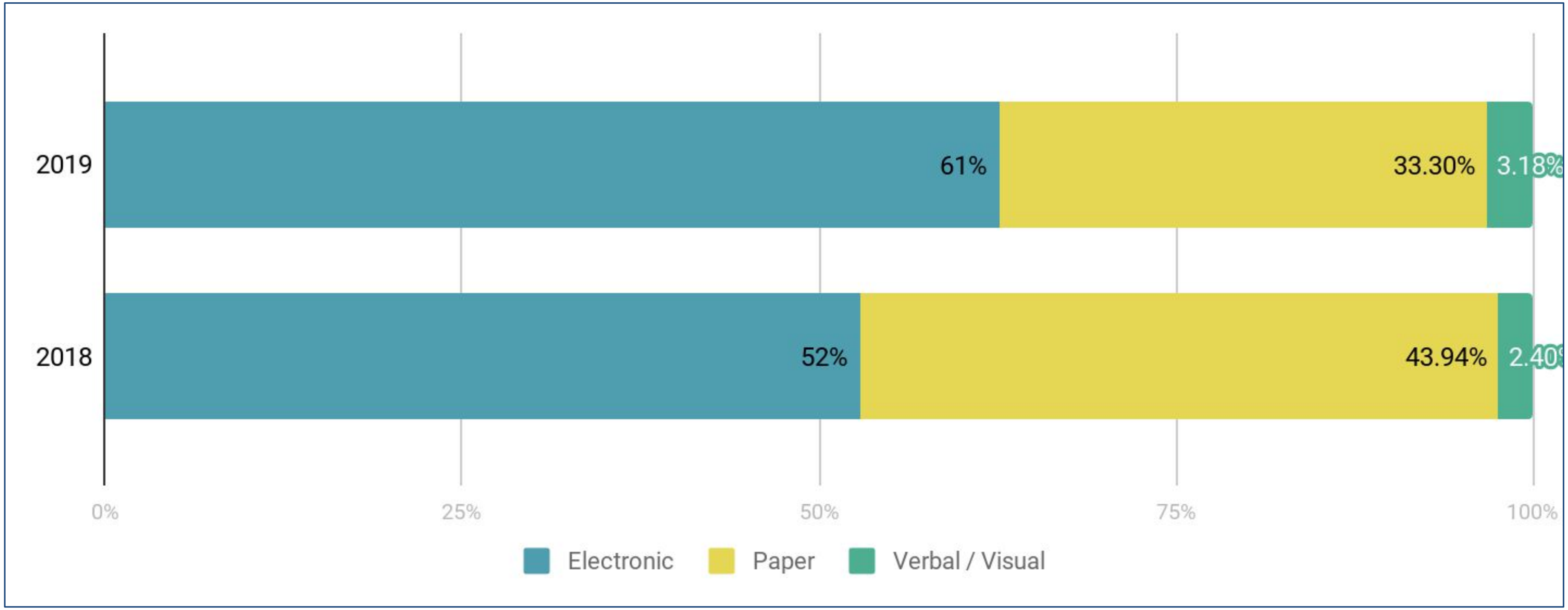
- **Incident:** Unauthorized disclosure of personal information where multi-factor risk assessment is performed to decide whether it is a Breach
- **Breach:** An incident that requires notification to impacted individuals
- **Occurrence Date:** Date the incident took place
- **Discovery Date:** Date the entity became aware of the incident
- **Notify Date:** Date of first notification to regulators or individuals

Incident lifecycle time periods

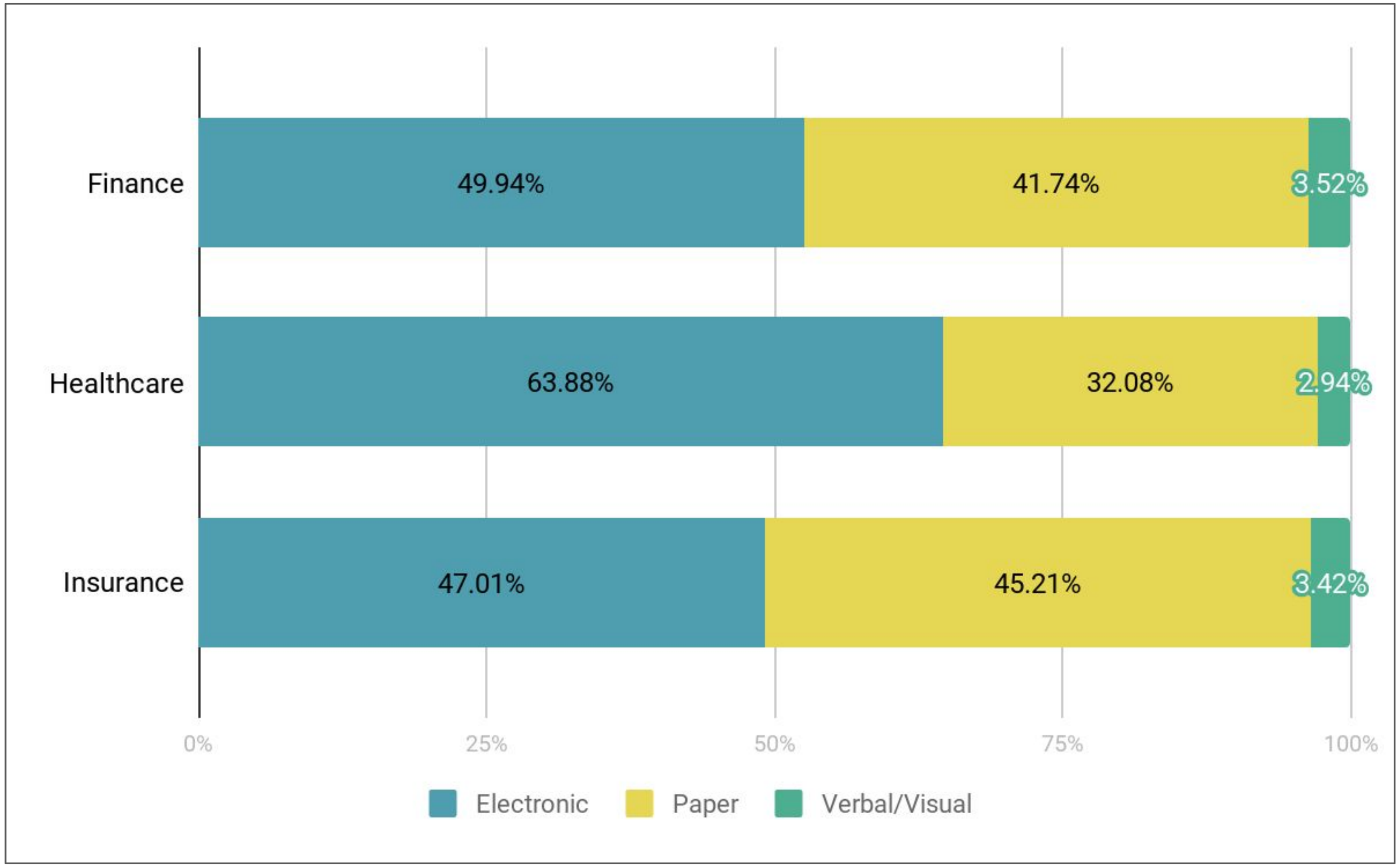


2019 BakerHostetler Report:
Occurrence to discovery: 66 days
Discovery to notify: 56 days

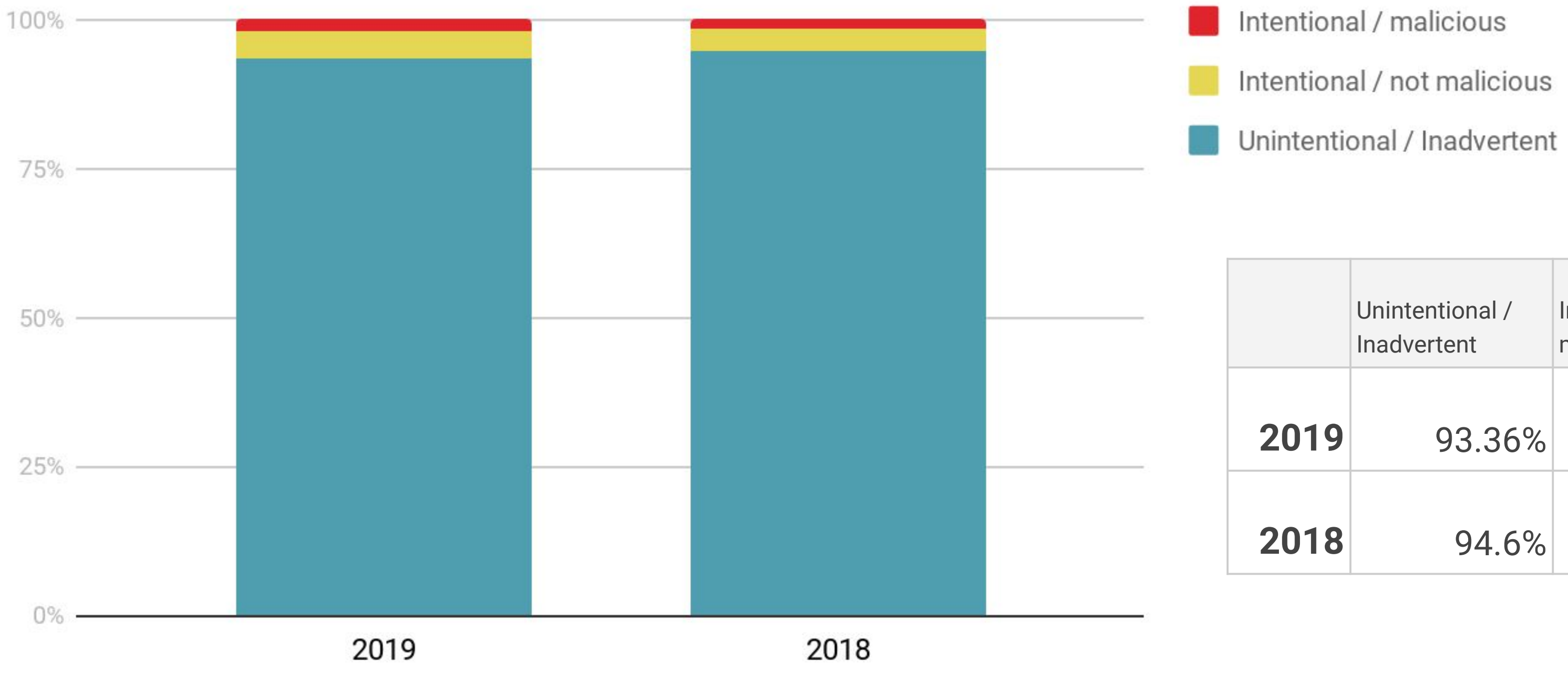
Electronic vs. Paper vs. Verbal/Visual



Electronic vs. Paper vs. Verbal/Visual - Industry Breakout



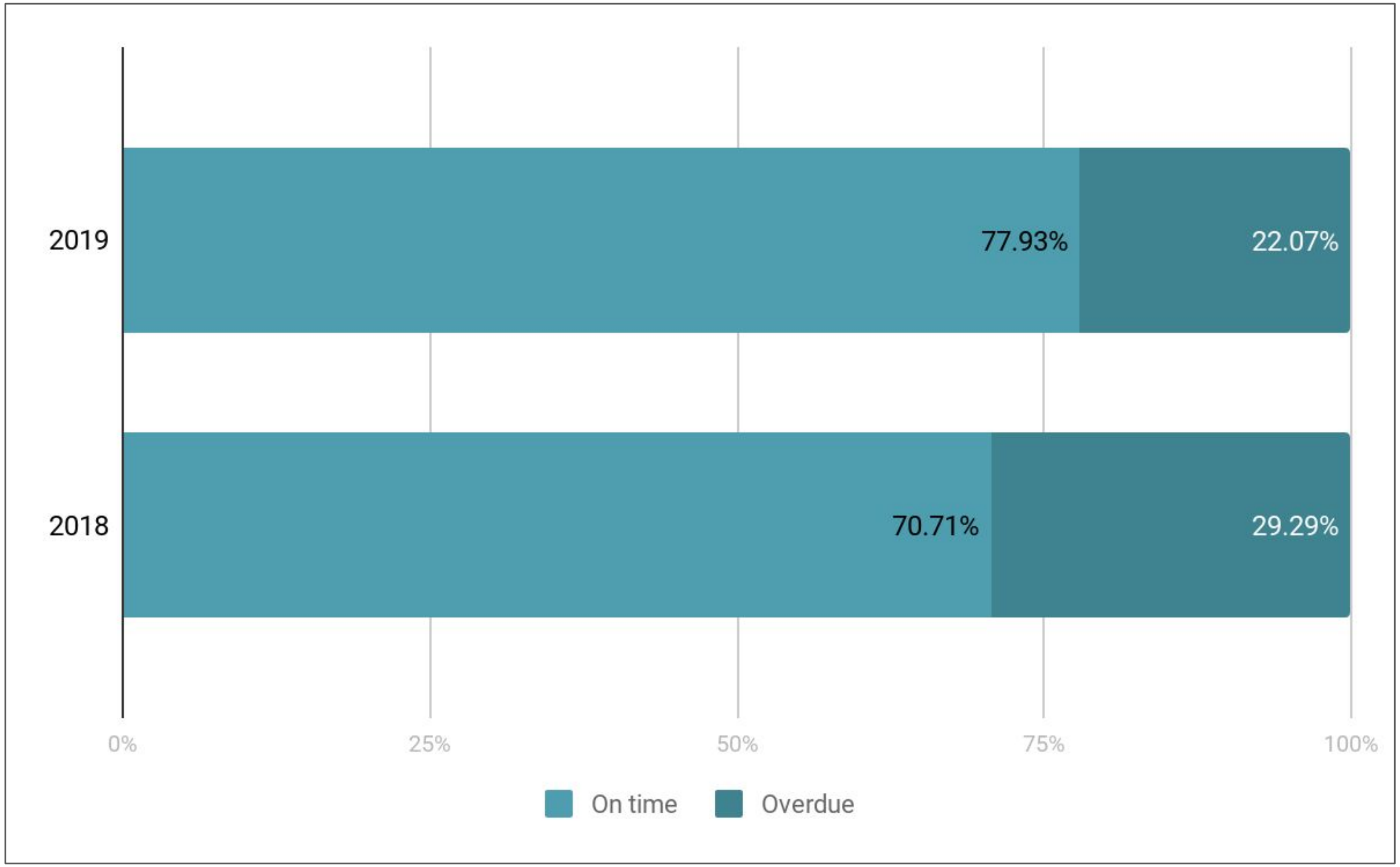
Malicious vs. non-malicious



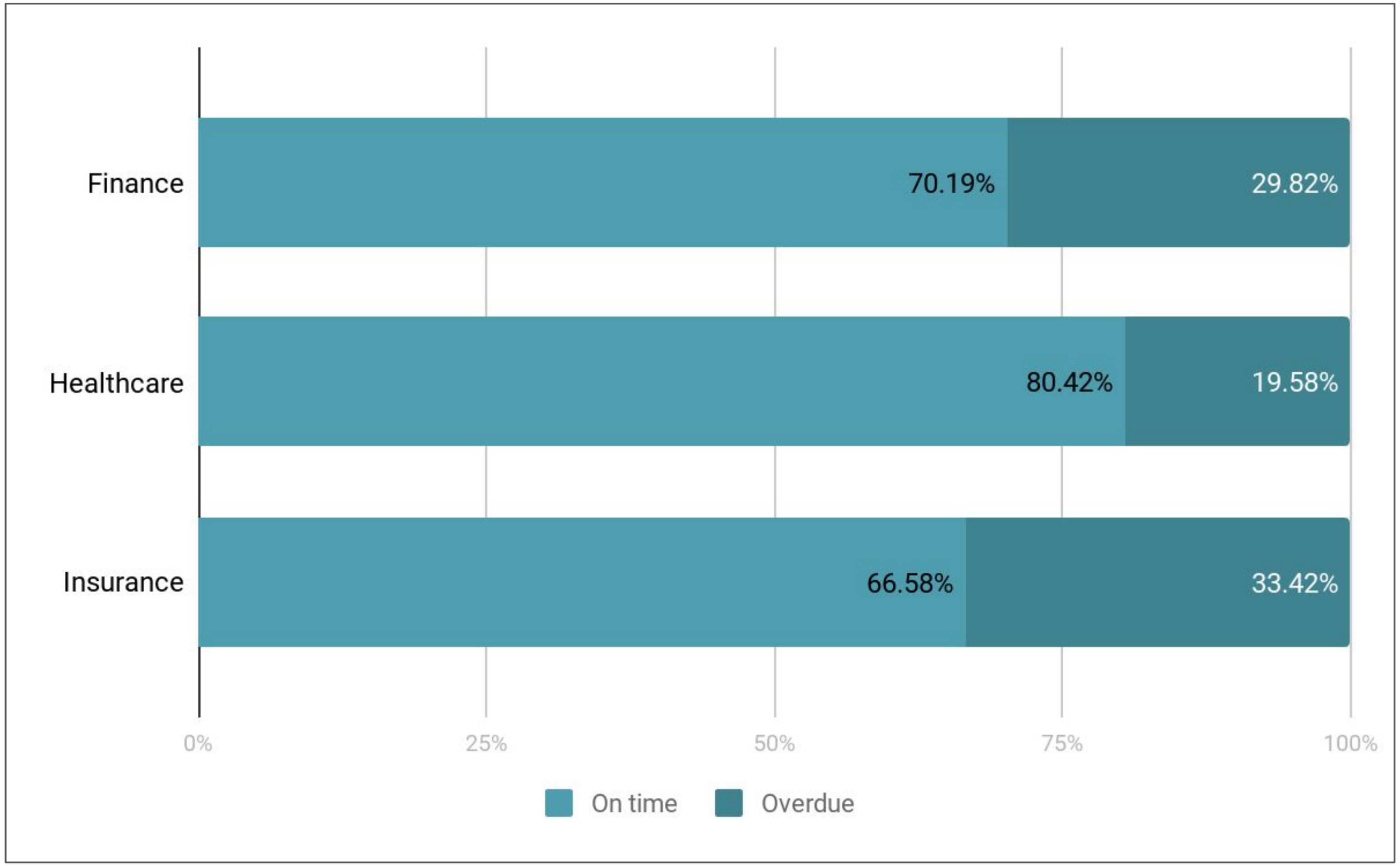
	Unintentional / Inadvertent	Intentional / not malicious	Intentional / malicious
2019	93.36%	4.84%	1.8%
2018	94.6%	3.67%	1.7%

- **The majority of incidents are unintentional or inadvertent**
- Regardless, there is a legal obligation to justify the decision, as well as document and demonstrate consistent risk assessment

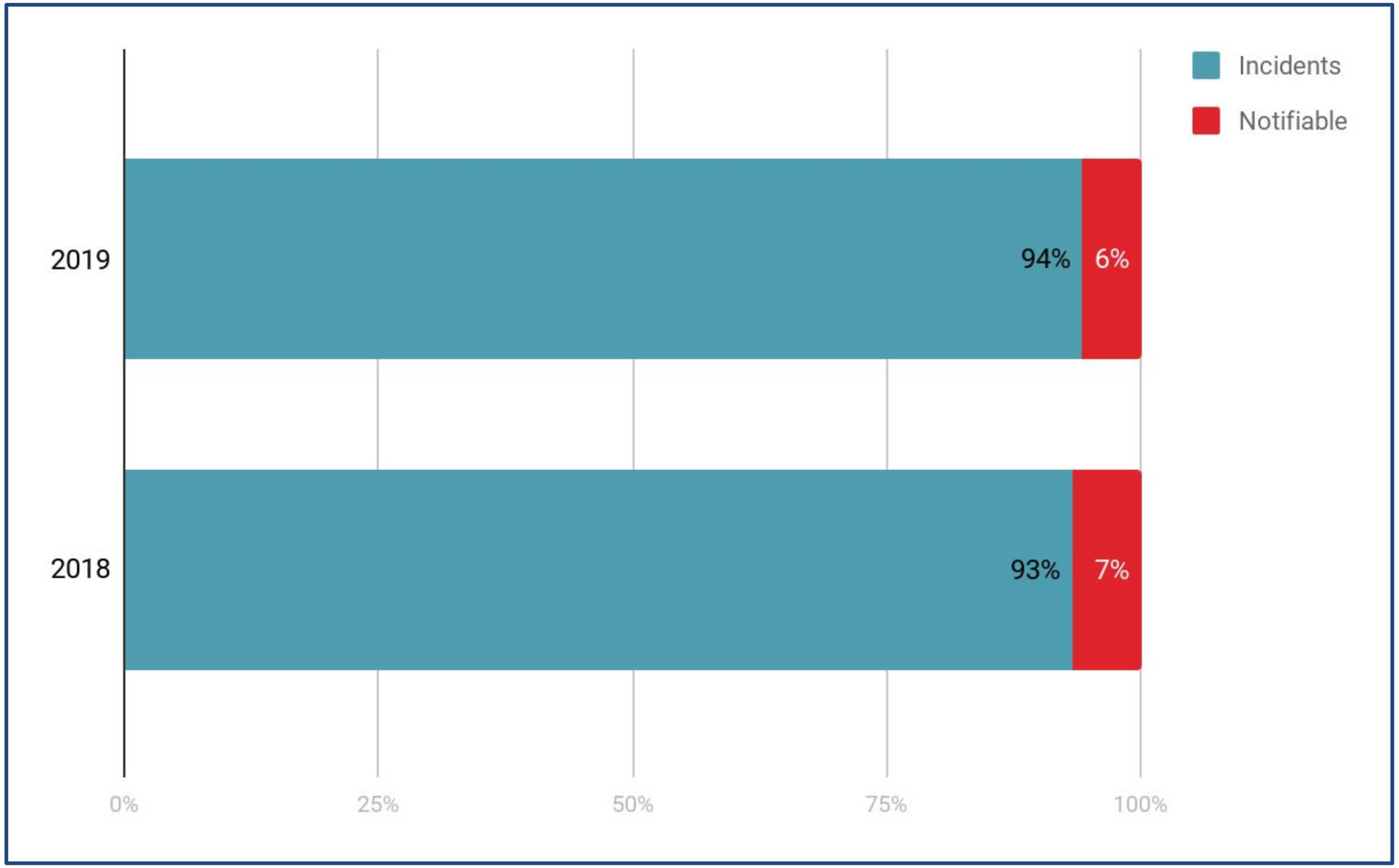
On time notifications



On time notifications - 2019 industry breakout

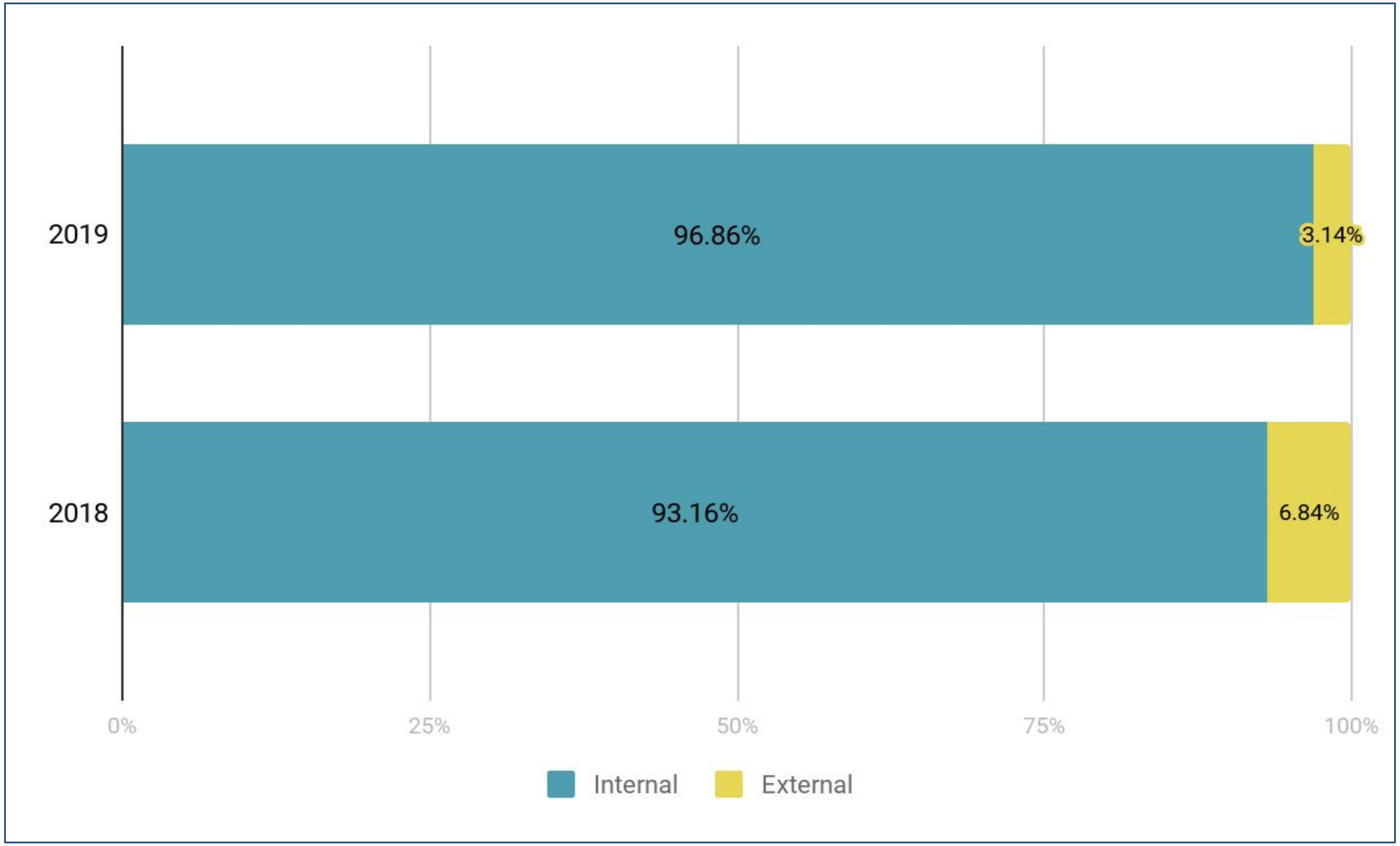


Is there a reasonable notification rate?



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

Internal vs External (third parties)



Actionable insights - Practical use cases

Actionable insights

- Focused training programs & awareness campaigns
- Discover areas where additional controls made to certain business processes are needed
- Uncover policy violations that have occured
  - pinpoint policies that need to be revised or created
- Identify business units where additional resources are needed
  - Develop a task force and/or accountability within the business units
- Review contracts with vendors

Quick tips for getting started

- Think about format & consider the audience
- Think about the story the data tells
- Pull out insights and conclusions that can be drawn based on the data
- Consider determining “normal run ranges” to identify when process anomalies may have occurred
- Maintain real-time metrics and dashboards (this will make it easier when needing to report to board and executive level)
    - Per month, per quarter, per year - look for seasonal trends & triggers
- Start small. Focus on a few metrics, get feedback, then expand
- Document actions taken as a result of the metrics to demonstrate business value/reduced risk over time

Attributes of a mature incident response program

Consistent	Objective	Timely	Defensible
Same incident risk profile but varying notification decisions look questionable and draw attention to a program that is lacking the necessary maturity.	Notification decision should be based on multi-factor risk assessment compliant with data breach regulations, not how you feel at the time or the climate of the environment.	An entity must notify individuals & regulators within varying but specified timeline to be compliant with breach notification laws & contractual obligations (in some cases, within 24 - 72 hours).	It is critical to document your incident risk assessment and the rationale behind your notification decision to notify or not notify.

Privacy Incident Benchmarking Report Available This April

How does your incident response program stack up to others?

Sign up to receive the inaugural report!

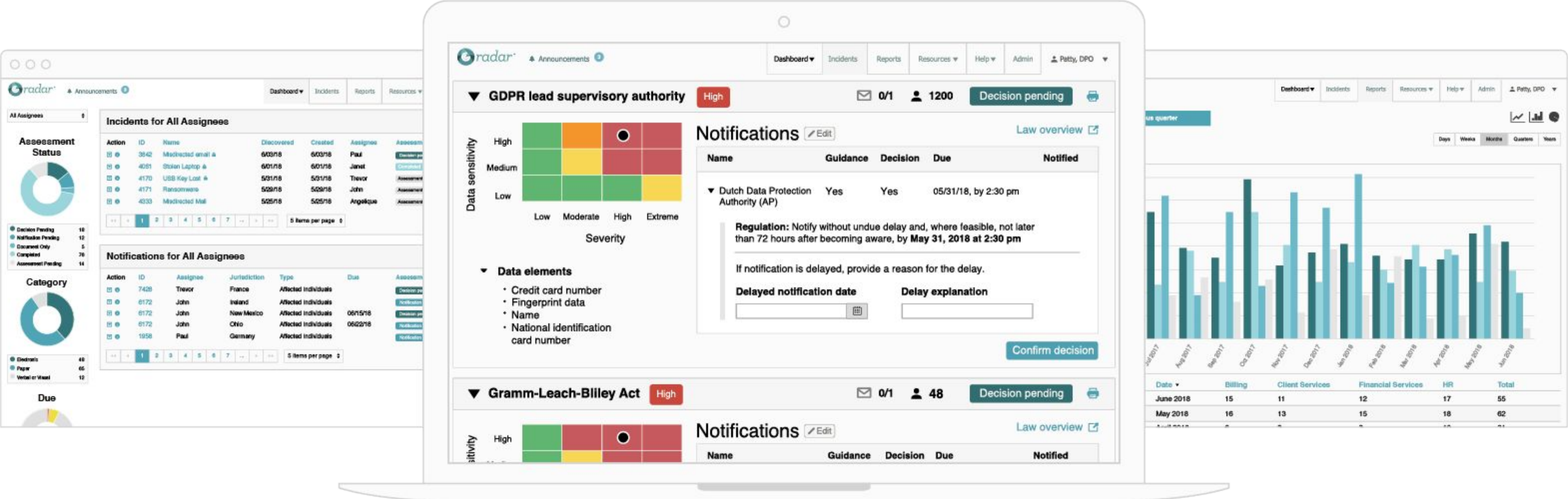
GET THE REPORT

www.radarfirst.com/benchmarking-report

Simplify compliance with automation

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

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



Incidents for All Assignees

Action	ID	Name	Discovered	Created	Assignee	Assessm
	3842	Misdirected email	6/03/18	6/03/18	Paul	Decision pe
	4051	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 pe
	6172	John	Ireland	Affected individuals		Notification
	6172	John	New Mexico	Affected individuals	06/15/18	Decision pe
	6172	John	Ohio	Affected individuals	06/22/18	Notification
	1958	Paul	Germany	Affected individuals		Notification

GDPR lead supervisory authority High

Data elements

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

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

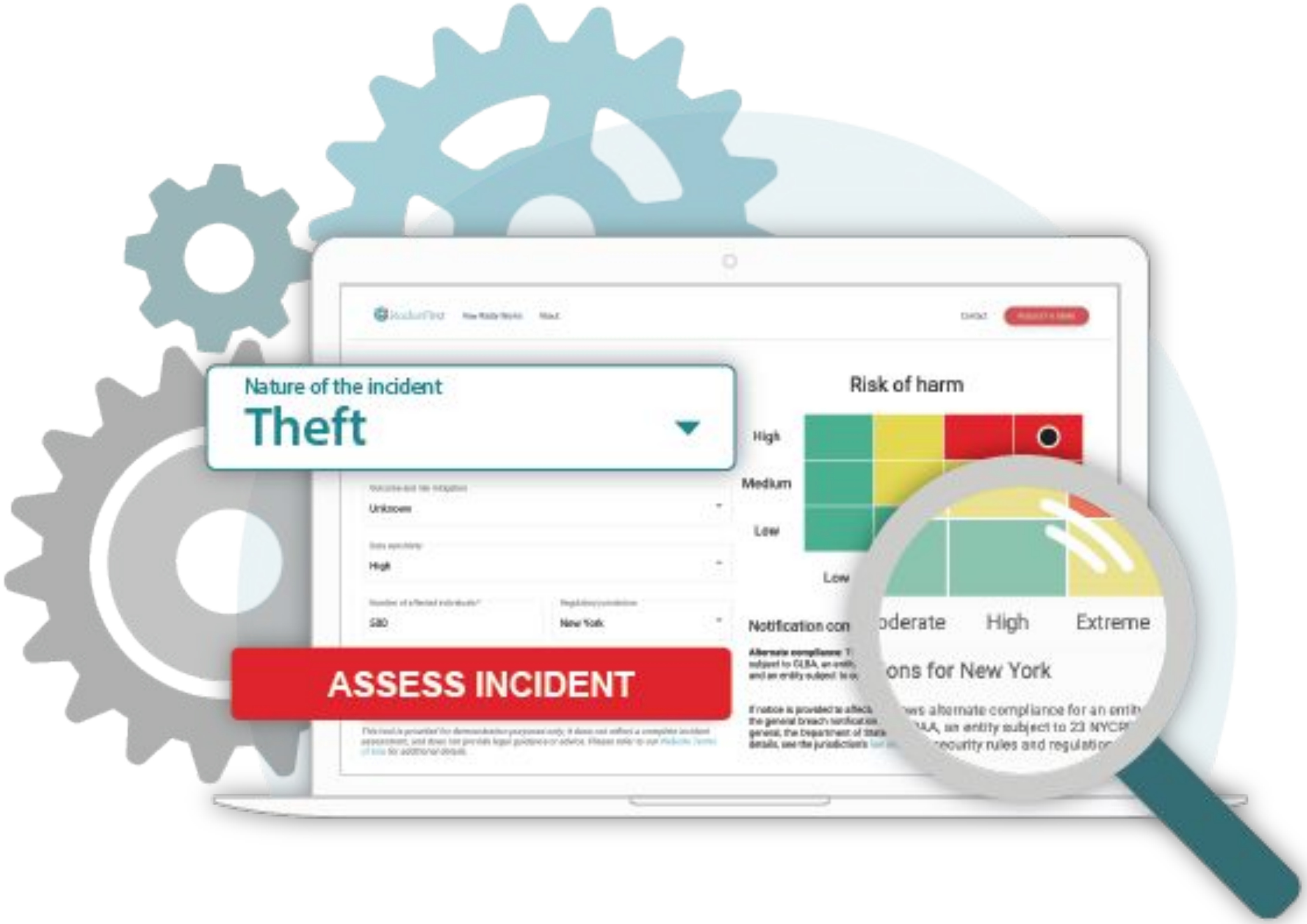
Gramm-Leach-Bliley Act High

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

Radar Breach Guidance Engine Simulator



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

ASSESS AN INCIDENT

breach-engine.radarfirst.com

Questions & Answers

Host:

Dave Cohen
CIPP/US, CIPP/E
Knowledge Manager
IAPP
dave@iapp.org

Speakers:

Mahmood Sher-Jan
CHPC
CEO & Founder
RadarFirst
mahmood@radarfirst.com

Michelle Wraight
CISM, CRISC
Director & Global Head of Privacy Automation
BNY Mellon
michelle.wraight@bnymellon.com

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: privacy@radarfirst.com iapp

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:

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 hour. 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: submit for CPE credits.

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