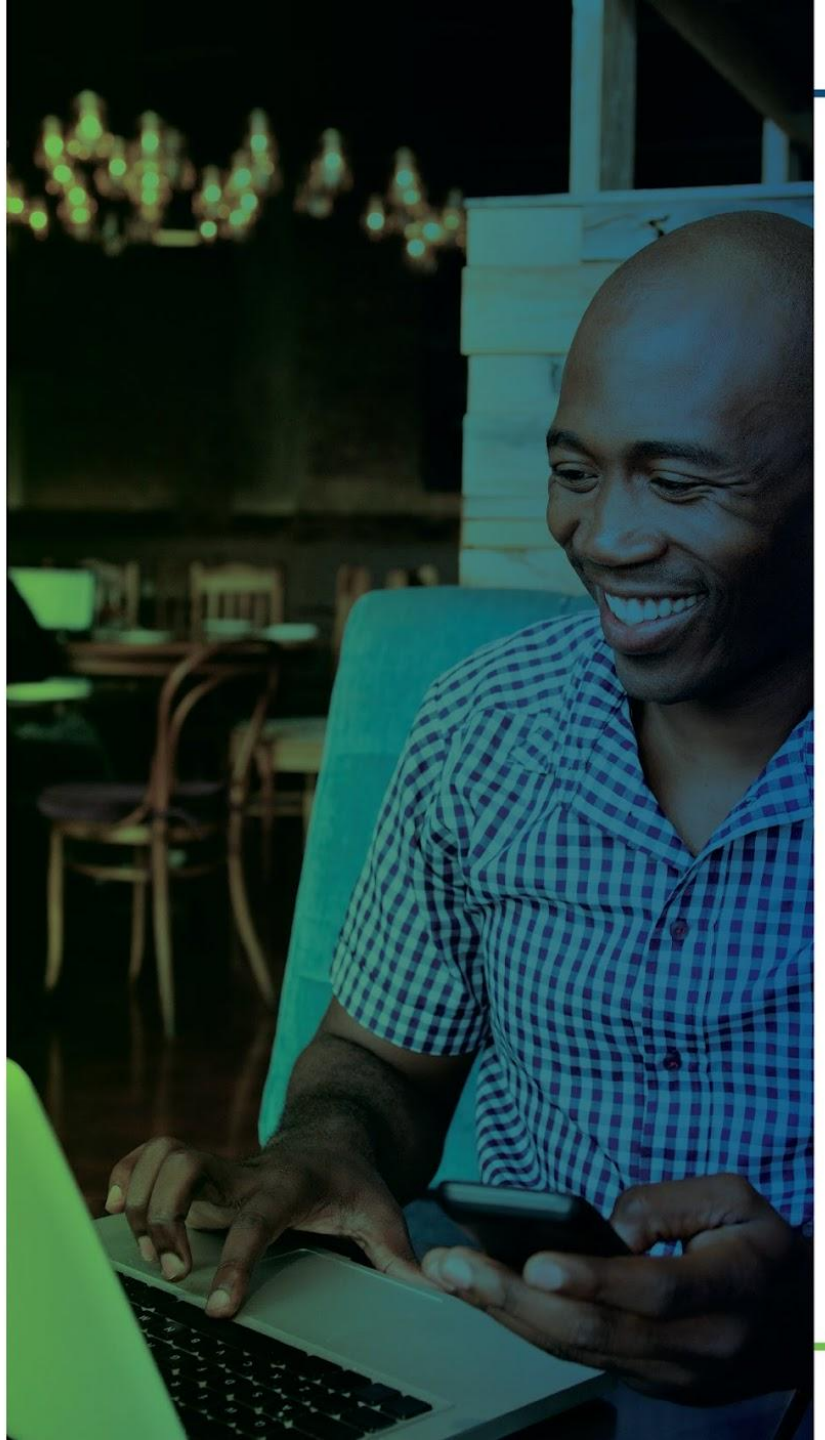


Highway to the regulation zone: The Intersection of cyber and privacy

Friday, 19/April/2024

10:00-11:00 PDT
13:00-14:00 EDT
19:00-20:00 CET

Welcome and Introductions

Panelists

Andrew Boden
Risk Outbound Product Manager
ServiceNow

Travis Cannon
Director
Integration Solutions
RadarFirst

Zelda Olentia
Lead Product Manager
Regulatory Analysis and Content
RadarFirst

Agenda

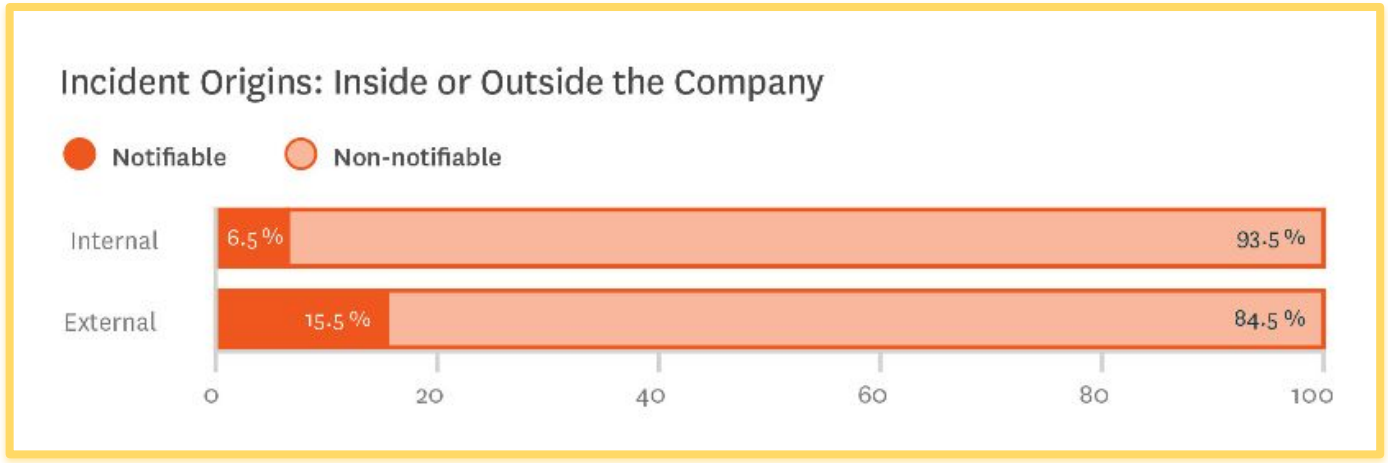
- Incidents will happen
- Keeping pace with regulatory requirements and reporting obligations
- Locate the intersection of cyber and privacy
- Demonstrate a collaborative and documented risk management plan

Incidents Will Happen[1]

93.5%
Incidents originated from **human error**

3.3X
Growth in **complex incidents** over the past 5 years

2.5X
Increased notification risk when incidents **initiate with a 3rd party**



[1] RadarFirst, *2024 Privacy Incident Management Benchmarking Report*, https://www.radarfirst.com/resources/2024-privacy-incident-management-benchmarking-report/

Top 5 Priorities for Legal & Compliance Leaders in 2024[2]

1. Expand legal and compliance impact on the enterprise
2. Strengthen third-party risk management (TPRM) programs
3. Develop a strategy that keeps pace with new regulatory requirements
4. Ensure guidance balances risk with business benefit
5. Create employee-tailored compliance training

[2] Gartner, *Top 5 Priorities for Legal and Compliance Leaders in 2024*, https://www.gartner.com/en/legal-compliance/trends/top-priorities-legal

Thoughts on Cyber Rule Making

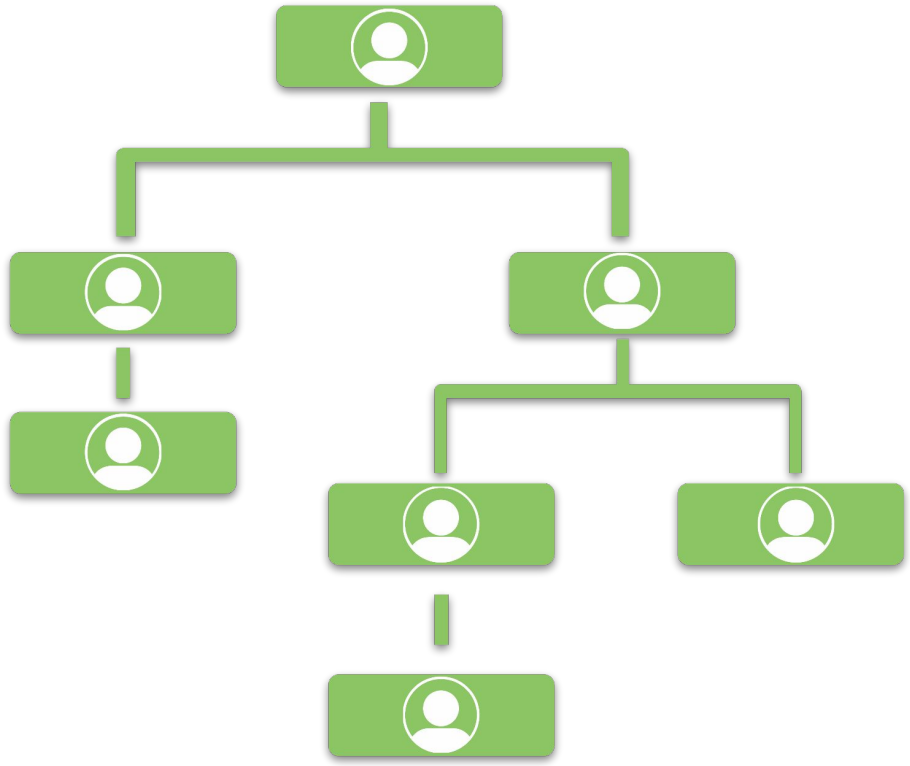
- When a company determines that it has experienced a material cybersecurity incident - **you have 4 business days to file a 8-K form with the SEC**
- "Materiality" is fact & context specific - **the same incident may be material for one company, and not material for another**
- Procedures for **assessing, identifying, and managing material risk** for cybersecurity threats:
  - Operations integrated into overall risk management system
  - Third parties engaged with company cybersecurity management
  - Processes to monitor risk from cybersecurity threats associated with third-party service providers

Cyber and Privacy Convergence

- Businesses will continue to collect our data
- Reliance on third parties to augment provided services
- Expanding definitions of PI
- Increasingly complex regulatory landscape creates new, overlapping cyber security and expanded data breach notification rules
- Cyber incidents and privacy data breaches will occur

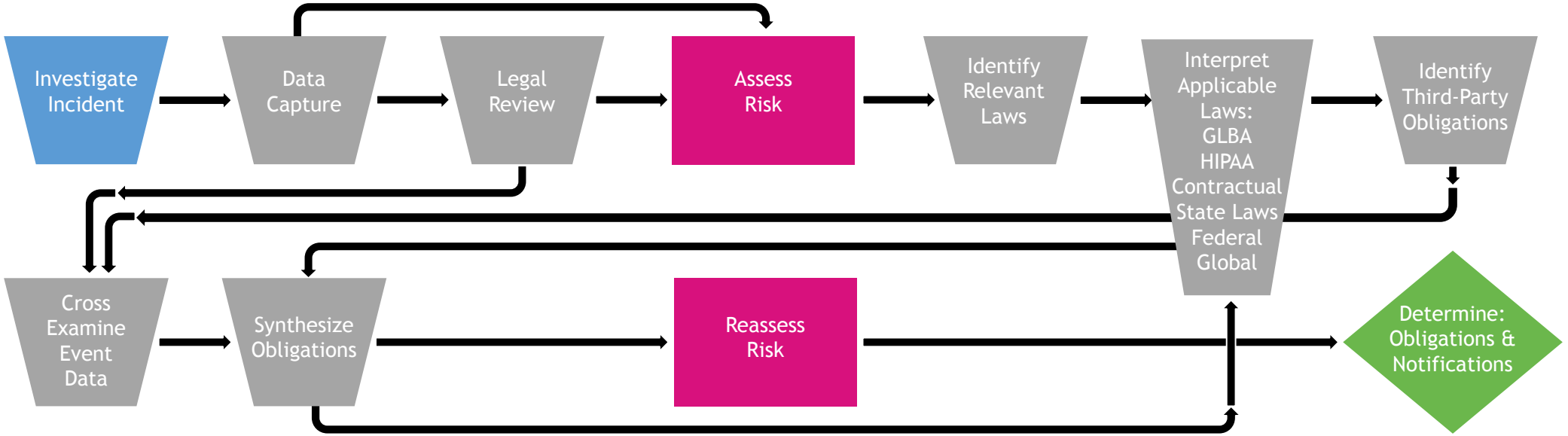
Organizational Response to Cyber and Privacy Convergence

- Compliance and Privacy report to Legal about half the time[3]
- InfoSec might report to CIO or somewhere else in the technology organization (66%), to another member of the C-Suite (27%) or to the CEO (7%)[4]
- Other stakeholders are all over the organization
- Incident Management must be responsive, coordinated, and aware



[3] Source: Association of Corporate Counsel 2022 Survey
[4] *Source: Ponemon Institute*

BEFORE: Risk assessment is inconsistent and laborious



Challenges to efficiency:

- Evolving regulations and obligations
- Inconsistent assessment and decision-making
- Missed obligation timelines
- Insufficient audit documentation
- Do more with less

AFTER: Streamlined incident assessment

Benefits of automation:

- Consistent decision-making with documented outcomes
- Scale operations and increase efficiency
- Accelerate time to resolution
- Future-proof compliance for evolving obligations
- Streamline collaboration organization-wide

Demonstration

ServiceNow | Privacy Case Management with servicenow

Radar® Privacy | Privacy Case Management integration with RadarFirst

ServiceNow Privacy Case Management Integrated with RadarFirst

Employee

Employee Center:

Report a privacy case

API Integration

ServiceNow solutions

3rd Party solutions

Integrations

Privacy Case Mgmt. Workflow

Privacy Case:
Business App
Security Breach

Triage & Investigate

Resolve

Post Case Review

Close

- Investigations & assessments
- Identify Impacted/ related areas such as Policies, Regulations, IT Assets, BUs
- Gather evidences & observations

- Initiate remediation and preventative measures
- Track regulatory violations to their lodgment

- Analyze the causes & consequences of the case
- Identify & manage issues related to impacted areas to eradicate the causes

Collaboration:

Evidence & resolution plan

Employee

IT

RadarFirst

Automating privacy case risk assessment and get clear, actionable notification obligations in seconds

HR

Legal

Demo

ServiceNow | Privacy Case Management with servicenow

servicenow | RadarFirst

© 2024 ServiceNow, Inc. All Rights Reserved. Confidential.

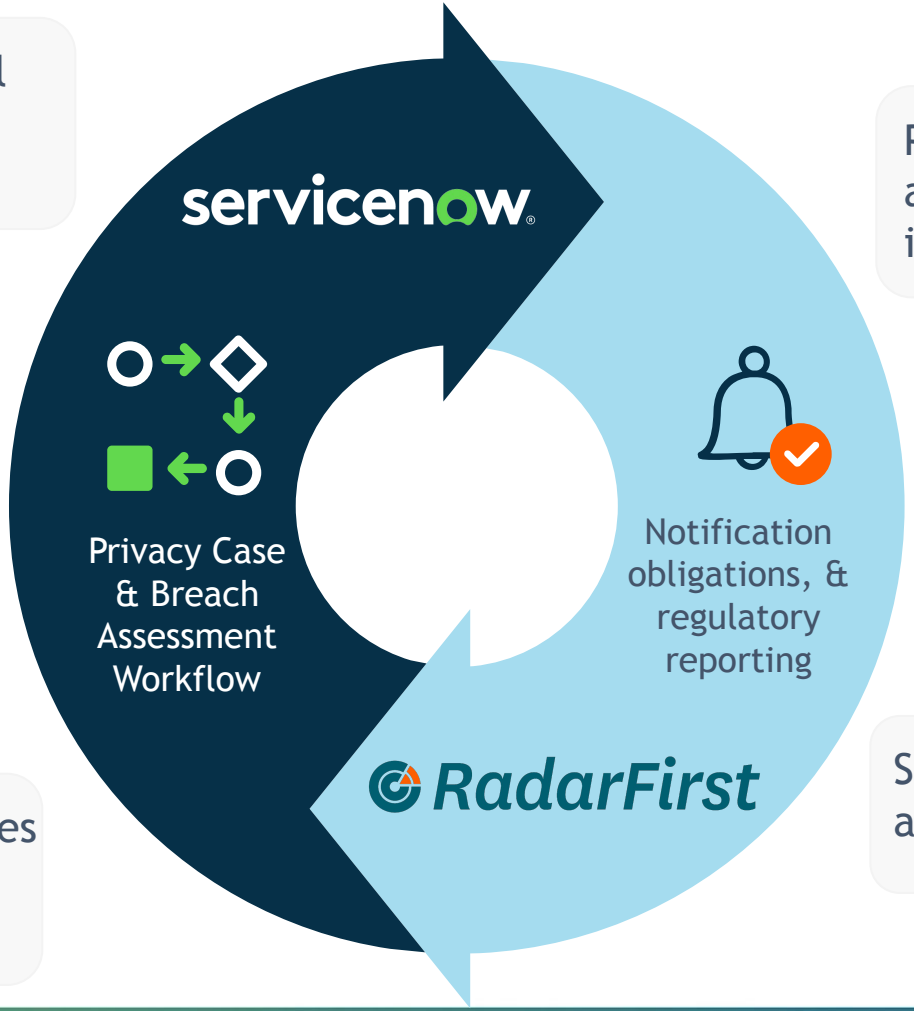
ServiceNow Privacy Case Management Integrated with RadarFirst

Identify and document critical details of privacy cases from various sources

Triage, Investigate and Identify impact radius
(Policies, Regulations, IT Assets, BUs)

Manage tasks across teams
(Security, HR, etc.) with SLAs to handle data breaches

Analyze the causes & consequences to plan and execute post case review process



Perform instant risk assessment to assess risk of harm to impacted individuals, your Org.

Highlight risks - Applicable privacy regulations, notification requirements, & timelines

Suggest resolution & corrective action & notification

How Do We Get Started?

- Start small to achieve early wins and create positive momentum.
- Create a regular cadence of reporting progress and focus on reporting results, not just activity. Clear KPIs are critical.
- Get buy-in/sponsorship from executives and keep them informed of early wins.
- Don’t forget to think/act horizontal.

Keep the conversation going!

SCAN ME

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://iapp.questionpro.com/t/AOhP6Z2Rdu

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/A, 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:

livewebconteam@iapp.org