RadarFirst

2024

PRIVACY INCIDENT MANAGEMENT

Benchmarking Report

Data to Build Trust and Reduce Enterprise Risk

Welcome

A word from leadership

In today's digital age, maintaining customer trust depends on how effectively organizations protect personal information and manage privacy incidents. As leaders in our respective fields, it's our responsibility to not only abide by the regulations that protect our customers but to continually improve our efforts to reduce risk and provide transparency for how sensitive data is managed.

This year's benchmarking report highlights the key trends and best practices in privacy incident management, providing valuable insights for organizations looking to enhance their operational capabilities. It also showcases how RadarFirst's patented Radar® Privacy technology has helped privacy-minded organizations streamline their incident management processes to reduce the risks associated with data breaches.

This report demonstrates that through consistent, automated incident management, organizations can effectively quantify risk, mitigate potential financial and reputational damages, and demonstrate their commitment to protecting their customers and stakeholders.

I encourage all organizations to use this report as a tool to enhance their risk management strategies and to see the value that RadarFirst can bring to their GRC efforts. Together, we can continue to raise the bar for privacy incident management and protect the trust of our customers.

Sincerely,

Don India
Chief Executive Officer

Through years of building program maturity, the privacy industry has become a beacon for others to develop assessment and reporting frameworks to mitigate risk. As a group, privacy leaders have helped demonstrate the value of viewing each incident as part of a comprehensive understanding of organizational risk, helping to better manage data and position our organizations for success.

This approach to comprehensive risk management requires collaboration among stakeholders to identify, remediate, and report incidents as they occur. Organizations that can operationalize risk management in this way can turn the inevitable security events, privacy breaches, and their overall risk posture into a strategic advantage in the eyes of customers, regulators, and investors–but not without taking full accountability for how incidents are managed.

We're pleased to report that Radar® Privacy continues to be crucial in facilitating collaboration, thereby reducing risks and effectively managing privacy incidents. The data presented in this benchmarking report highlights the success of Radar® Privacy in helping our customers improve their privacy incident management processes as well as their ability to adapt to new regulations.

I invite you to read this benchmarking report and discover how Radar® Privacy can help your organization reduce risk, improve incident response, and stay compliant, whether you are a current RadarFirst customer, or considering solutions for streamlining and collaboration in your privacy functions. I am confident that the findings will not only be insightful but also reinforce the value of investing in a solution to automate intelligent decisions.

Sincerely,

Lauren Wallace
Chief Privacy Officer & General Counsel

Executive Summary

Notifiable incidents (data breaches) increased to 7.1% in 2023

This is their highest percent of total since RadarFirst started publishing this report in 2018.

Large, complex privacy incidents have increased 3.3x since 2018

Incidents involving 1000 or more individuals typically span multiple state and/or jurisdictions — each with unique obligations and timelines.

Third Party incidents have 2.5x notification rate

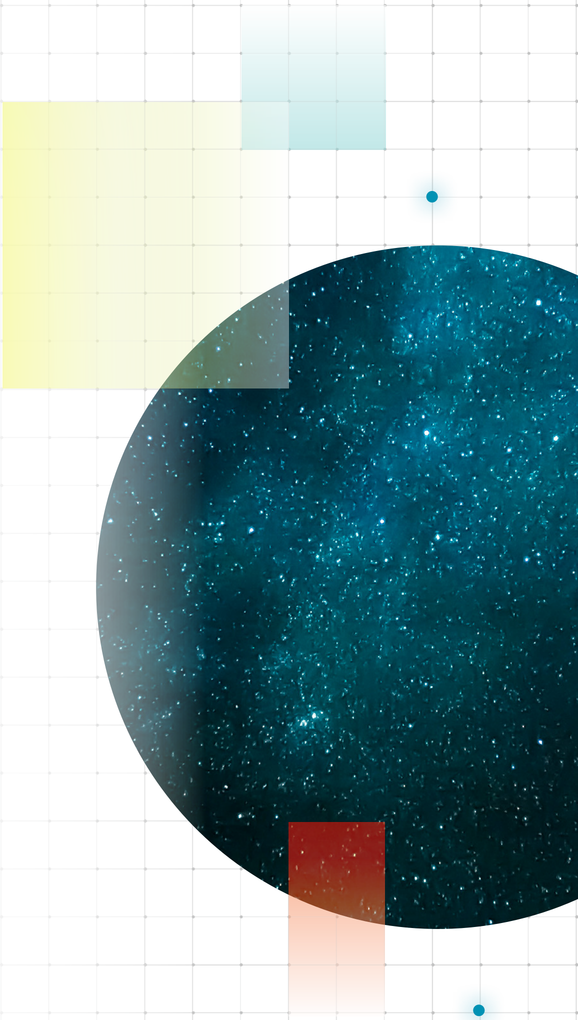
Third Parties augment staffing and expertise needs, but partnership comes with a **2.5x increase** in the rate of notifiable obligations.

Intentional events increased in 2023

An unwanted trend that brings with it more notifiable events.

Contents

Data Breaches: A Harsh Reality



Data breaches are a growing concern in global news. For companies that rely on data collection to gain competitive advantages, heightened attention from regulators brings new pressure to meet compliance obligations as part of an overall risk strategy.

While it can be exciting to read headlines about the latest actions of cybercriminals, no company is immune to unintentional privacy incidents. The best way organizations can mitigate the risk is through routine incident response, sound third-party management, and consistent privacy awareness training.

When a breach occurs, mature organizations know that having an objective approach that yields a clear picture of their notification obligations is critical to reducing risk and maintaining trust with customers and regulators. At its core, effective incident management is built on clear, consistent processes to assess risk and determine notification obligations.

This report explores the importance of assessing each privacy incident as part of the bigger picture of preparedness. By establishing a consistent, repeatable, and documented process to scale privacy operations, you too can build trust, bolster organizational resilience, and reduce risks associated with data breaches.

Key Terms

INCIDENT

An unauthorized disclosure of personal information where an automated privacy risk assessment is performed to decide whether it is a notifiable breach.

NOTIFIABLE BREACH

An incident that, under applicable laws/regulations, requires notification to affected individuals, a federal and/or state agency, a regulatory agency, and/or the media. Additional notification may be required by contract to a third party (e.g., upstream customer).

Privacy incidents will happen

This year's report shows that most incidents happen due to human error, often the result of people simply performing their job. When incidents begin at one of your downstream third parties, the notification risk increases by a factor of 2.5.

7.1% of all assessed incidents (independent of intent) warranted notification. This increase from 6.2% in 2022 is the highest notifiable rate since we started collecting data in 2018.

93.5%

incidents originated from

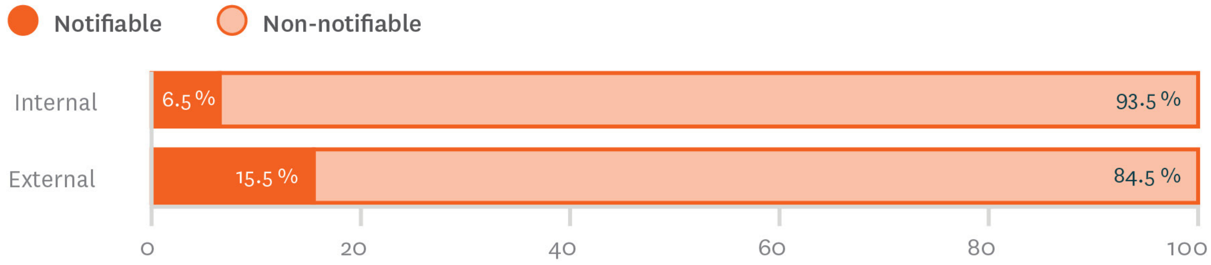
human error

2.5X

increased notification risk when incidents

initiate with a 3rd party

Incident Origins: Inside or Outside the Company



Key Terms

EXTERNAL INCIDENT

An incident caused by a third-party data processor, business associate or service provider.

INTERNAL INCIDENT

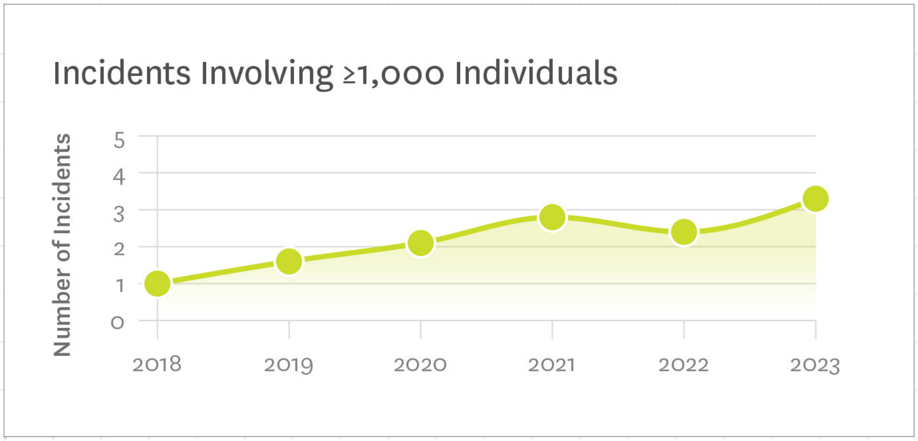
An incident that originates within your organization due to intentional or unintentional employee action.

UNINTENTIONAL INCIDENT

An incident caused by human error resulting in an unauthorized disclosure of personal information.

Complexity x Scale

This year we're adding a new report to demonstrate the increase in large incidents, which involved 1,000 or more individuals. Larger incidents will likely involve an increase in the number of applicable jurisdictions requiring risk assessment as well as the number of notification reporting timelines required to meet compliance.


Incidents Involving ≥1,000 Individuals

The number of large incidents increased 3.3x since 2018 (chart normalized to 2018).

Jurisdictions

In 2023, the average incident assessed included 5 jurisdictions, but not necessarily the same 5 each time. These numbers peak for the insurance industry that averaged 9 jurisdictions per average incident and financial institutions which averaged 7.

5

● ● ● ○ ○
● ● ○ ○ ○

average number of
jurisdictions per incident for all industries

9

● ● ● ● ●
● ● ● ● ○

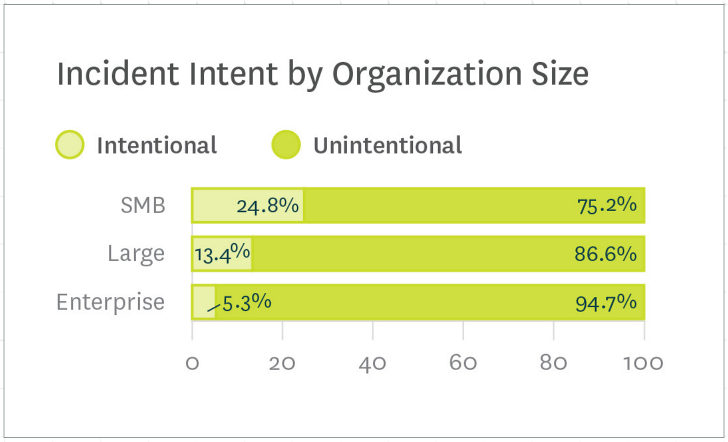
average number of
jurisdictions per incident for Insurance industry

Intentions:

Unintentional or Malicious?

Since we began reporting in 2018, **unintentional human error** has been the leading source of privacy incidents.

On average, 7.1% of all assessed incidents are notifiable (up from 6.2% in 2022) — the highest level since 2018. Possibly driving up this notification rate is the fact that Intentional incidents have increased in 2023, bringing with them increased notification rates.


Incident Intent by Organization Size

Smaller organizations have more intentional incidents.

The larger the enterprise, the more likely it is they provide privacy awareness training. Regardless of organization size, the main cause of breaches is due to human error.

Key Terms

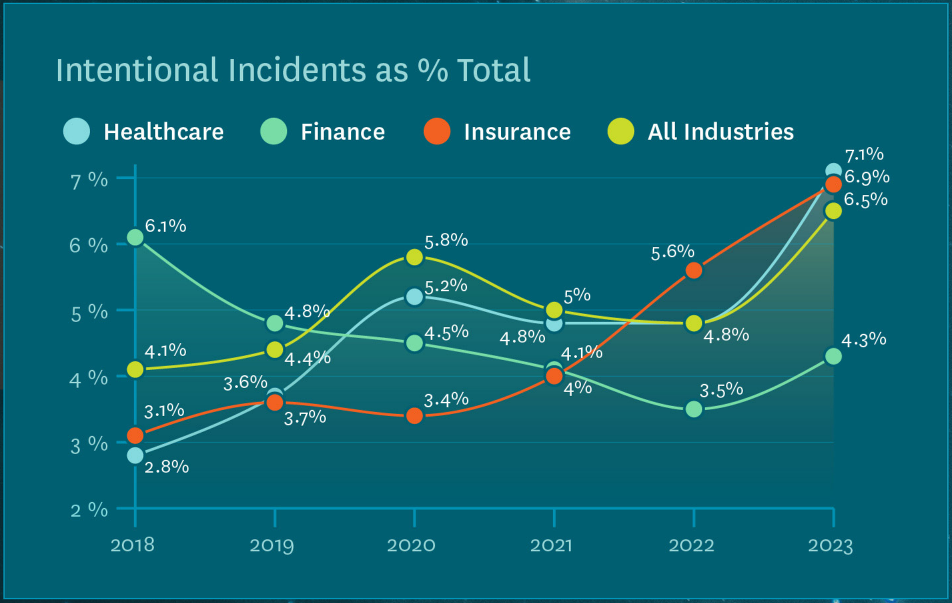
INTENTIONAL INCIDENT

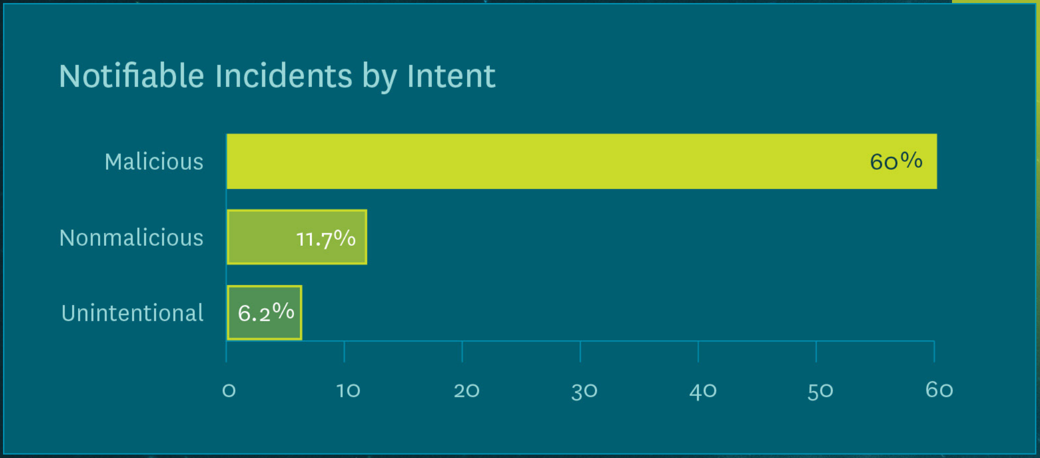
An incident caused by unauthorized access to personal information, with or without harmful intent to the individual(s) and/or the organization.

ORGANIZATION SIZE

Small and Medium-Sized Business (SMBs): <1,500 employees
Large: 1,501-10,000 employees
Enterprise: 10,000+ employees

Intentional incidents across all industries increased to 6.5% of total.

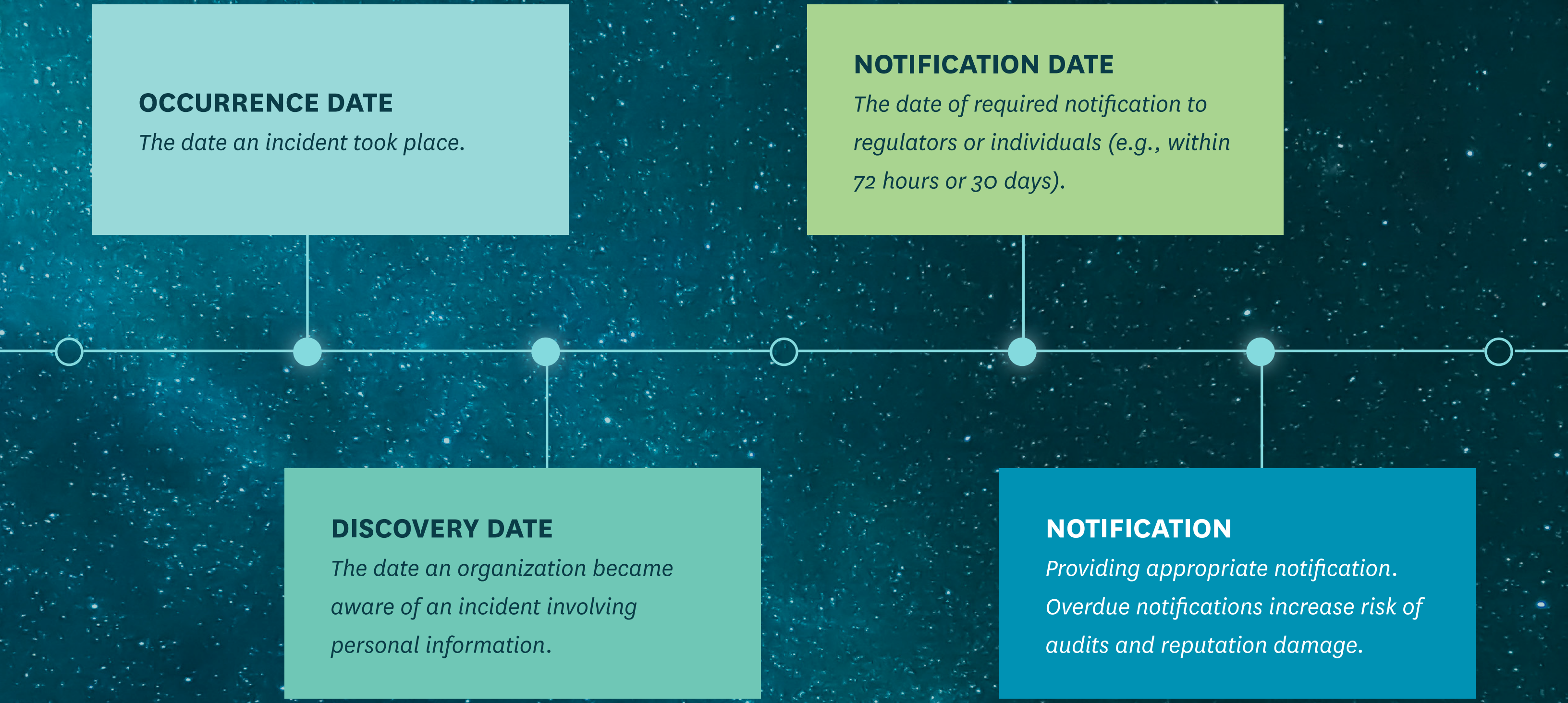

Intentional Incidents as % Total


Notifiable Incidents by Intent

For the first time intentional incidents increased across all industries in 2023, contributing to increased notification rates.

Key Takeaways

Human error and the expansion of third-party relationships to augment staffing will continue to increase organizational vulnerabilities. Establishing privacy training across an organization and being prepared with a repeatable, consistent, and documented approach to handling incidents is the most effective way to manage breaches and mitigate the impact.



OCCURRENCE DATE
The date an incident took place.

DISCOVERY DATE
The date an organization became aware of an incident involving personal information.

NOTIFICATION DATE
The date of required notification to regulators or individuals (e.g., within 72 hours or 30 days).

NOTIFICATION
Providing appropriate notification. Overdue notifications increase risk of audits and reputation damage.

Time Compounds Risk

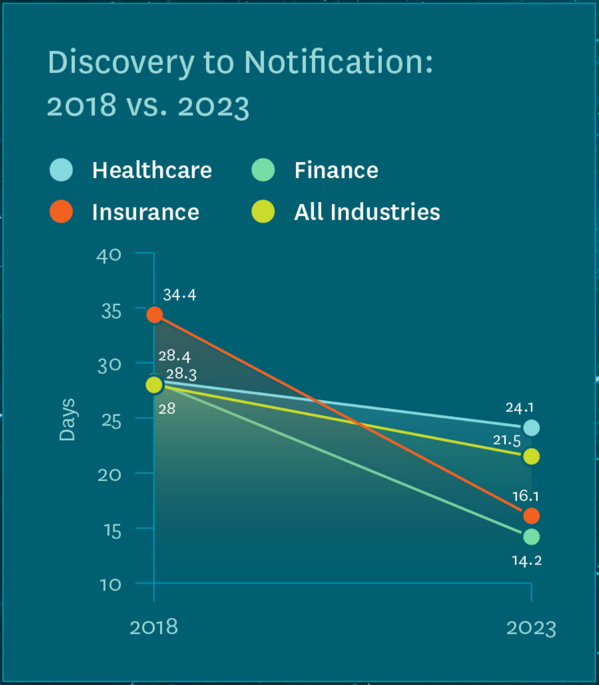
Once an incident is identified ("discovered"), the regulatory clock starts ticking. From that moment, privacy teams must act swiftly to comply with breach regulations and to notify the relevant authorities and individuals, making it critical for organizations to minimize the time between discovery and notification.

Organizations that leverage RadarFirst have seen efficiency gains in their discovery-to-notification processes over the past six years. For continued improvement, a discussion about overdue or on-time notifications is necessary to ensure that organizations are meeting their legal obligations and taking appropriate steps to mitigate the impact of a data breach.

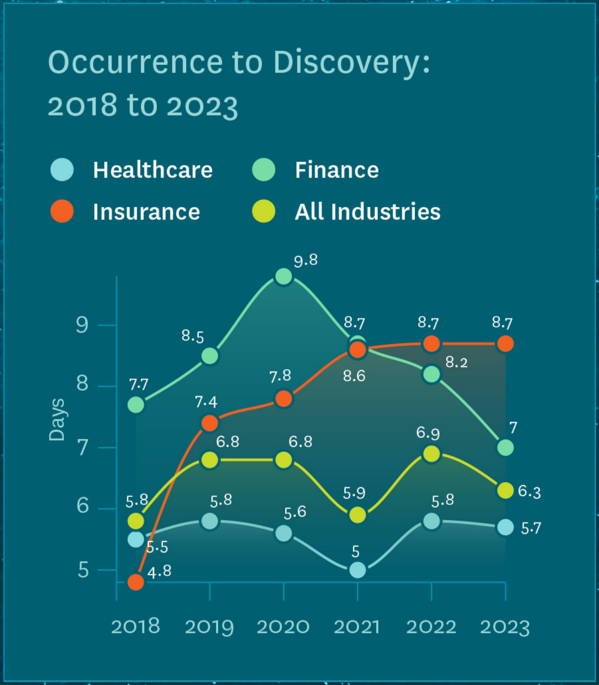
Overdue Notifications

Time is of the essence. **All industries took 21.5 days to first notification** after initial incident discovery (a decrease from 22.9 days in 2022). Discovery to Notification continues to decline with the use of Radar® Privacy. Discovery to Notification times vary by industry.

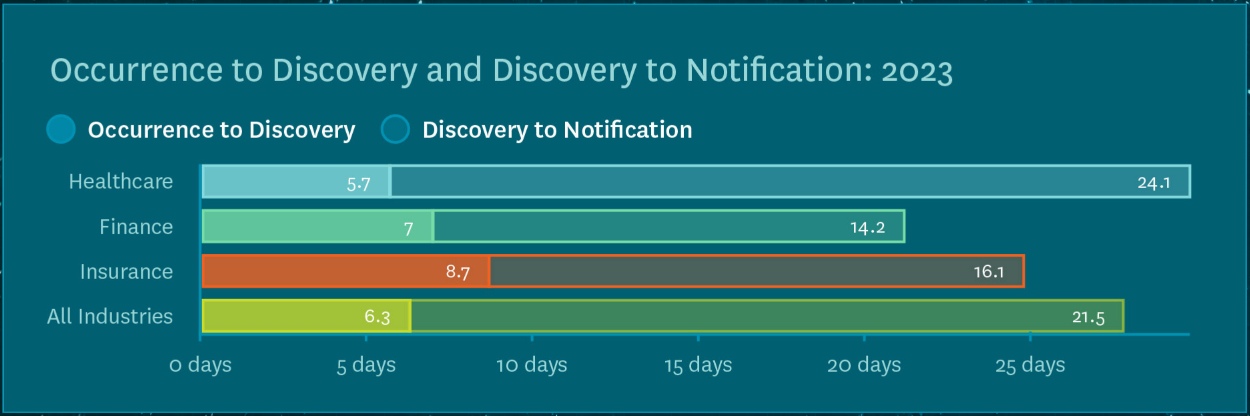
Radar® Privacy captures the incident timeline from Occurrence to Discovery, which took **an average of 6.3 days in 2023**. From the chart below, it's clear that incident discovery continues to be a challenge.



Discovery to Notification: 2018 vs. 2023

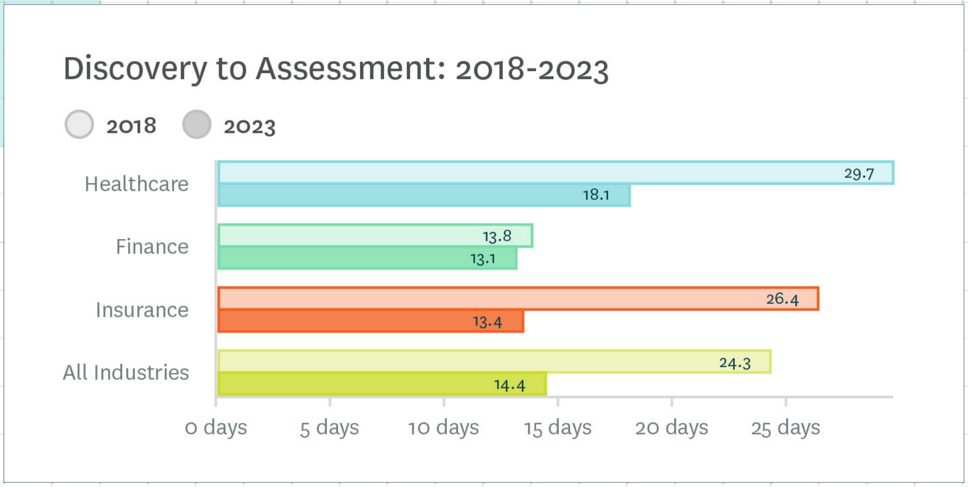


Occurrence to Discovery: 2018 to 2023

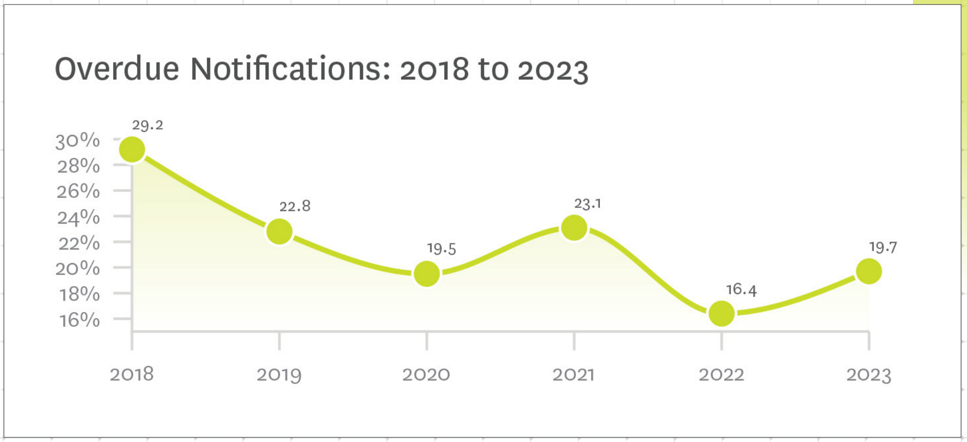


Occurrence to Discovery and Discovery to Notification: 2023

Radar® Privacy users have decreased time from discovery to first risk assessment by 10 days since 2018.


Discovery to Assessment: 2018-2023

Radar® Privacy has enabled a 33% reduction in overdue notifications.


Overdue Notifications: 2018 to 2023

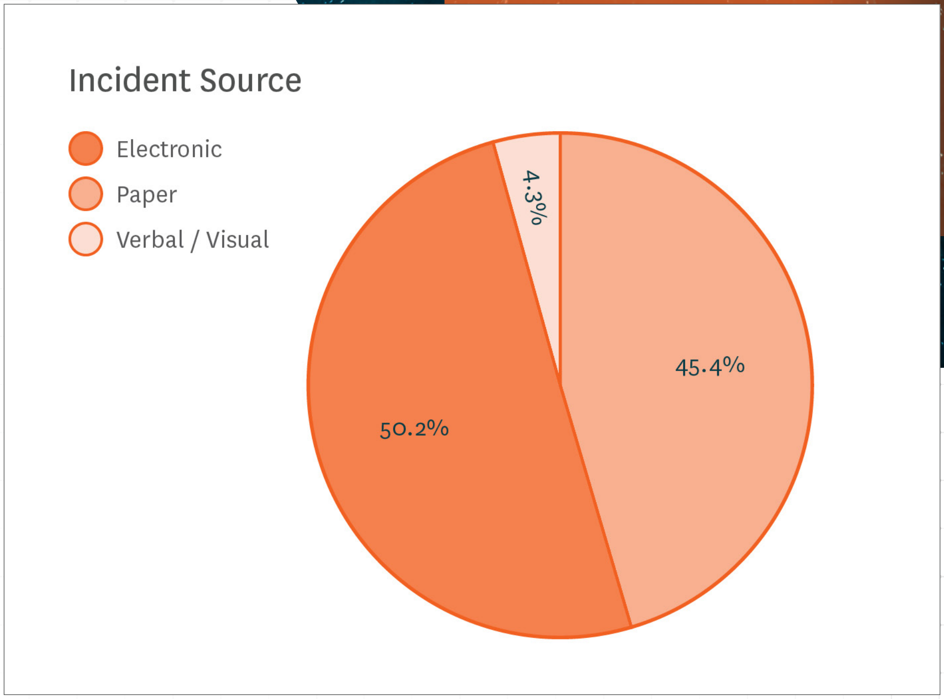
Key Takeaways

The longer an incident goes unresolved, the higher the risk of a damaging outcome. Radar® Privacy users have seen efficiency improvements since we began tracking this data. As an adjacent observation from data collected, Occurrence-to-Discovery timelines continue to be a challenge across industries.

The Privacy Incident Landscape

Every incident is unique. Understanding the nuances of an incident's origins — whether inadvertently emailed (electronic), accidentally displayed during a presentation (visual), inappropriately discussed (verbal), or improperly disposed papers — can help you mitigate future risk.

Total verbal/visual incidents are down 11% in 2023.



Key Terms

ELECTRONIC-BASED INCIDENT

An unauthorized disclosure of personal information via access to a database, email, or other electronic means.

PAPER-BASED INCIDENT

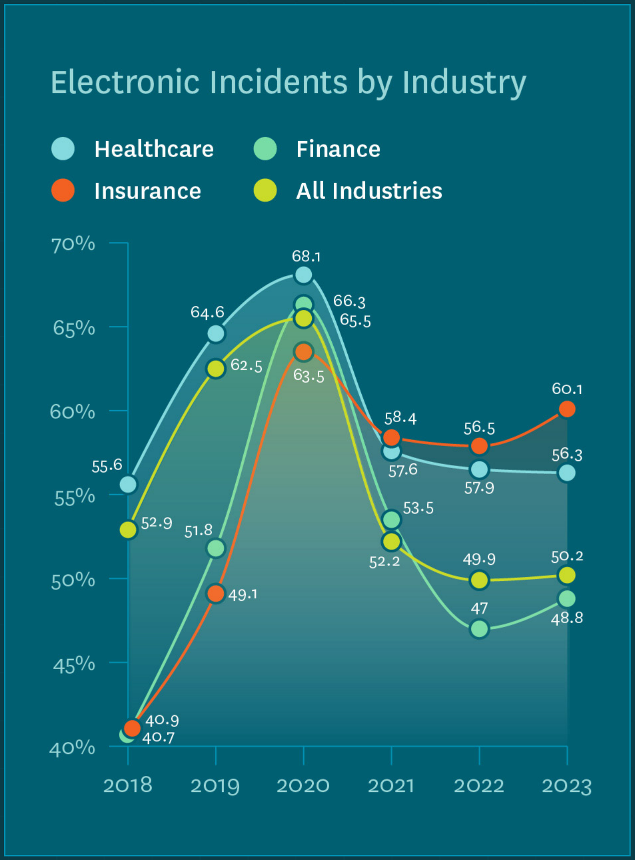
An unauthorized disclosure of personal information via printed documents.

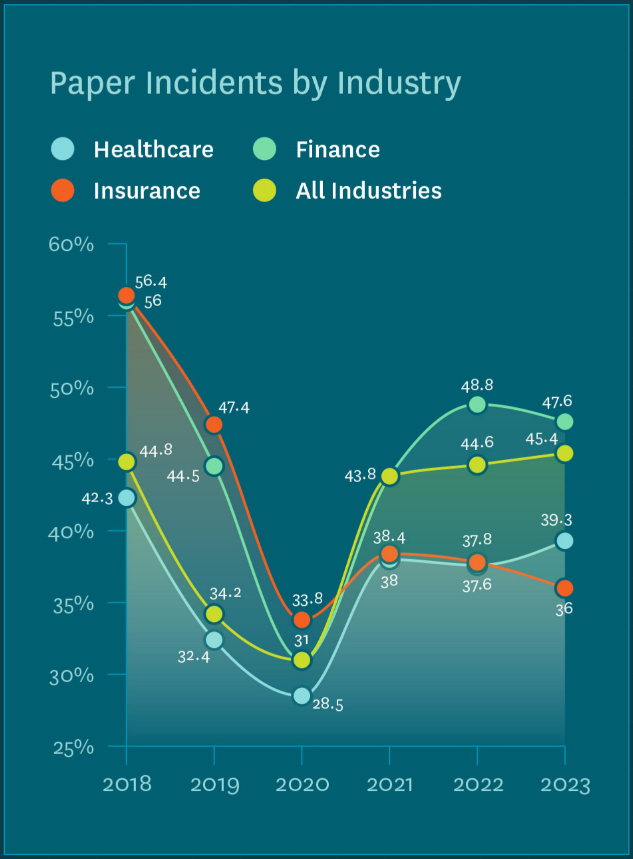
VERBAL/VISUAL INCIDENT

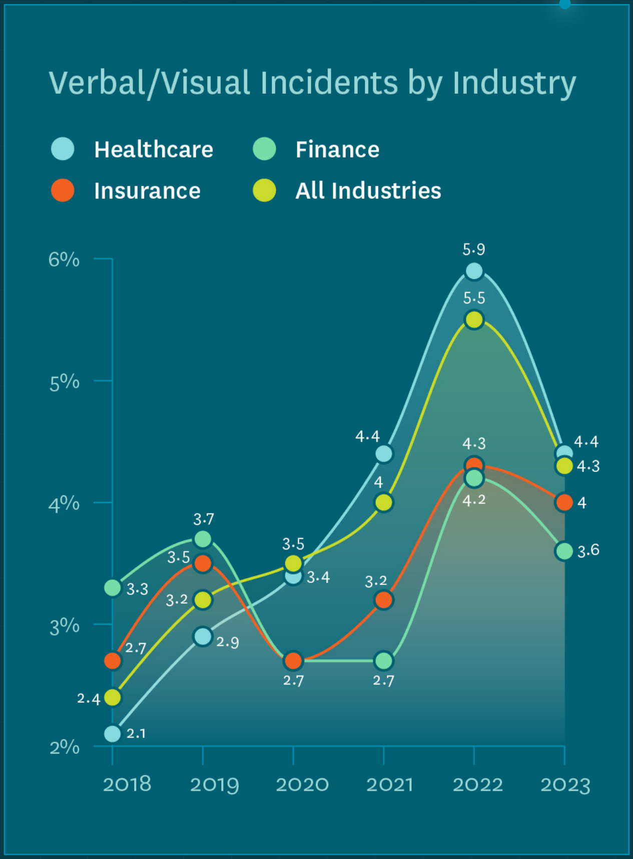
An unauthorized disclosure of personal information through spoken word or visual observation.

Source Trends by Industry

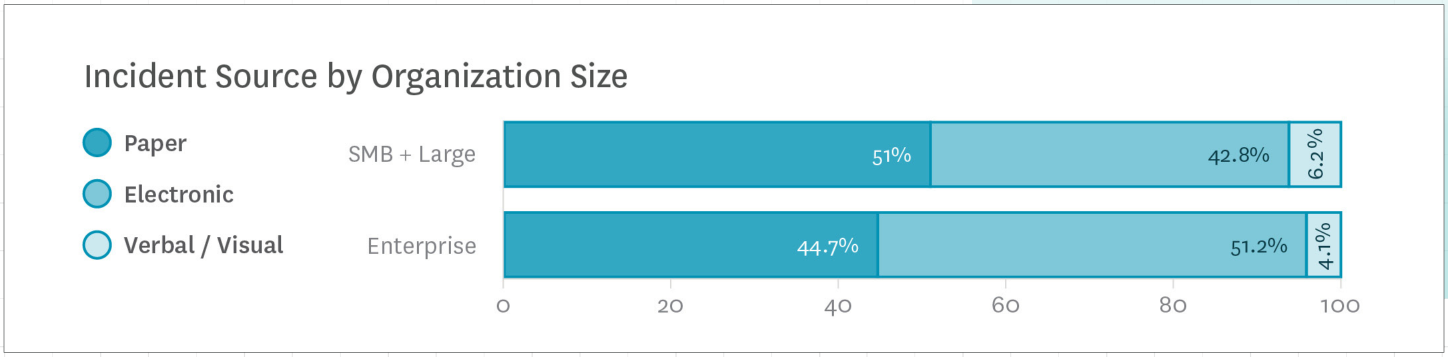
During the COVID-19 pandemic, organizations rushed to secure a newly remote workforce. At the height of the pandemic, this new change contributed to a decline in paper incidents but contributed to a spike in electronic incidents. When return-to-work protocols activated in 2022, verbal/visual incidents rose across all industries.


Electronic Incidents by Industry


Paper Incidents by Industry


Verbal/Visual Incidents by Industry

Enterprise organizations that have been able to operationalize privacy awareness training benefit from decreased verbal/visual-based incidents and paper-based incidents. However, due to increased data collection and third-party vendor relationships, electronic-based incidents claim a larger percentage of total incidents.



Key Takeaways

By increasing privacy awareness training and the need for immediate incident reporting, all companies could gain a better understanding of the importance and potential consequences of a privacy incident. This would lead to quicker mitigation and resolution of incidents. After all, incidents do not typically originate within the privacy department, thus it takes organization-wide understanding of their risks to escalate and remediate potential threats. This is especially crucial as time is not on the side of a company managing a privacy incident, and the longer it goes unresolved, the higher the risk becomes.

Resources

Digital Transformation Guide for Privacy Incident Management

Future-proof your organization across four intersecting domains: technology, data, processes, and organizational change.

www.radarfirst.com/digital-transformation-for-privacy

Privacy Incident Management Software Comparison

See how the Radar® Privacy Intelligent Incident Management platform stacks up against workflow automation tools.

www.radarfirst.com/privacy-software-comparison

Privacy Team Tabletop Exercise

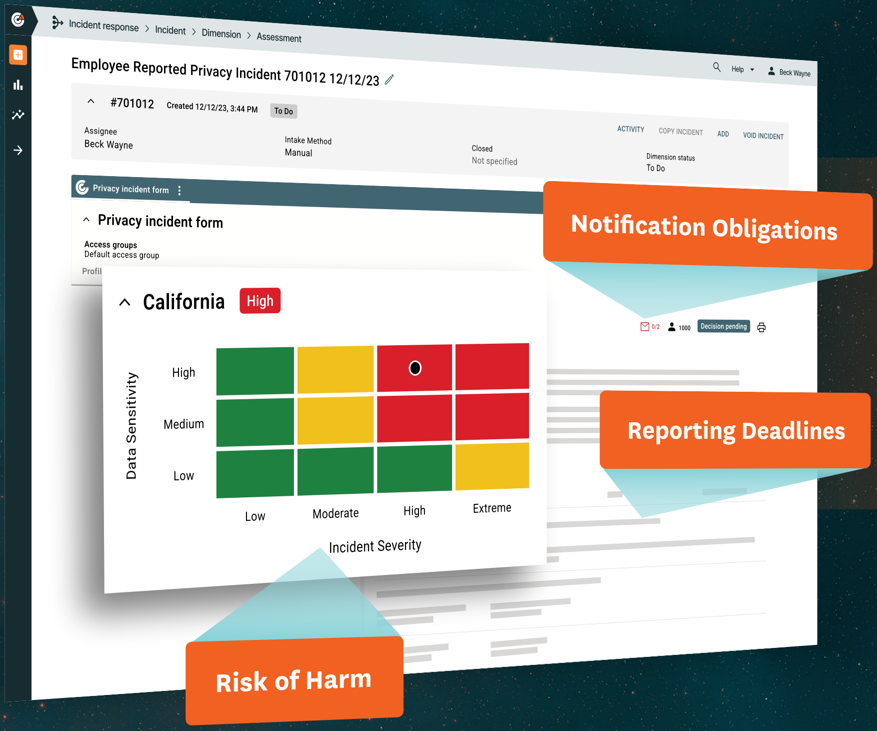
Practice incident management scenarios to prepare your team for when a breach occurs.

www.radarfirst.com/privacy-tabletop

Radar® Privacy

SEE RADARFIRST IN ACTION

Find out why RadarFirst customer loyalty is industry-leading



Incident response > Incident > Dimension > Assessment

Help · Beck Wayne

Employee Reported Privacy Incident 701012 12/12/23

#701012 Created 12/12/23, 3:44 PM To Do

ACTIVITY COPY INCIDENT ADD VOID INCIDENT

Assignee: Beck Wayne

Intake Method: Manual

Closed: Not specified

Dimension status: To Do

Privacy incident form

Privacy incident form

Access groups: Default access group

California High

Decision pending

Notification Obligations

Reporting Deadlines

Risk of Harm

Schedule a demo at:

radarfirst.com/radar-privacy-demo

About RadarFirst

RadarFirst offers SaaS solutions to simplify obligation decision-making as mandated by new and changing privacy and compliance regulations. The patented Radar® Privacy product is trusted by enterprises and organizations to automate privacy incident management and response for consistent, documented breach notification decisions. Radar® Compliance is a configurable rules and assessment engine, addressing cyber and compliance incidents, that offers organizations the ability to define their own notification triggers and obligations to stakeholders at every level, from federal regulators to board of directors to third-party obligations. The result is operationalized compliance, cyber, and risk notification obligations for intelligent notification decisions and collaborative risk management organization-wide. RadarFirst solutions help customers satisfy compliance, privacy, security, and legal regulations within their incident response plans.

Learn more at radarfirst.com

TOP WORK PLACES

The Oregonian OREGONLIVE