



2026

PRIVACY INCIDENT MANAGEMENT

BENCHMARKING REPORT

INSIGHTS FROM



www.radarfirst.com
info@radarfirst.com

INTRODUCTION

THE UPHILL SPRINT: FASTER RESPONSES, HIGHER STAKES

Privacy teams entered 2026 in a significantly different position than just a couple of years ago. Many of the bottlenecks that once slowed incident responses have been addressed. Discovery, assessment, and notification timelines have improved, reflecting years of investment in process, tooling, and organizational discipline.

But a faster response has not reduced risk. As teams move more quickly, the nature of incidents is changing. Malicious intent is rising as a percentage of the overall incident volume, and when incidents occur, they are more likely to escalate rapidly with significant regulatory, financial, and reputational consequences. The margin for error has narrowed. Teams are expected to move quickly and get it right the first time. The cost of a misstep has never been higher.

**SPEED ALONE IS NOT ENOUGH.
ORGANIZATIONS MUST MATCH
ACCELERATION WITH ACCURACY.**

At the same time, AI is reshaping privacy operations. It enables significant efficiency gains, but also introduces new threat vectors and governance challenges, amplifying both productivity and risk. This year, we will explore how organizations are adapting under these pressures and examine AI's growing role in greater depth in the Bonus Chapter: The Future of AI in Privacy.

The message is clear: speed alone is not enough. Organizations must pace accuracy with acceleration. Efficiency is no longer a competitive advantage; it is a prerequisite for operating in a faster, more complex, and increasingly unforgiving risk environment.

LEADERSHIP VIEWPOINT

Privacy incident management is entering a more demanding era. Organizations have made real progress in improving operational speed, cutting notification timelines, and streamlining response workflows. Those gains are reflected in this year's data, but speed alone is no longer enough. Incident volume continues to rise, with reported incidents up 11.6%, and malicious intent is growing faster as a percentage of overall incident volume. At the same time, artificial intelligence is reshaping privacy operations. AI offers meaningful efficiency gains, enabling teams to respond at scale, but it also introduces new privacy risks and governance challenges that cannot be ignored.

These pressures are driving increased investment. According to the latest Cisco 2026 Data and Privacy Benchmark Study, **38% of organizations now spend at least \$5 million annually on data privacy activities**, up from just 14% in 2024, **and a 171% increase in two years**. This growth reflects a broader reality: privacy incident management has become a core operational function.

Efficiency, in this environment, is no longer just a goal. It is a survival mechanism. Organizations that invest in solid processes and efficient, operationalized privacy incident management platforms are better positioned to manage double-digit incident growth, reduce exposure, and demonstrate defensible decision-making under regulatory and board-level scrutiny.

As AI becomes embedded in core operations, the need for structured, defensible incident response extends beyond traditional privacy events. The same operational discipline that enables organizations to manage privacy incidents at scale will be critical as AI-related incidents become part of everyday operations.

At RadarFirst, we see this shift firsthand. The most resilient organizations are those that prioritize consistency, automation, and clarity, building programs designed not just to respond, but to scale. This report reflects this evolution and provides a data-driven view into how leading teams are adapting.

We hope the insights in this report serve as both a benchmark and a guide as you navigate the year ahead. The terrain is steeper, the pace is faster, and the stakes are higher. Privacy incidents will increasingly involve automated decisions, scaled data flows, and cross-functional accountability. Organizations that operationalize structured, defensible incident management today will be better positioned to respond consistently to what comes next.



Zach Burnett
CEO, RadarFirst

KEY HIGHLIGHTS

- 1

Incident Volume is on the Rise

Privacy teams are facing sustained workload pressure. Incident volume rose again in 2025, increasing 6.41%, even among organizations using mature incident management programs, reinforcing that rising volume is a structural challenge and not an isolated trend.
- 2

Malicious Risk Is Accelerating

Although malicious incidents account for a small portion of total cases, their faster growth rate (+10.3%) points to a more challenging and higher-stakes risk environment.
- 3

Low-Frequency, High-Severity External Incidents

External incidents made up just 4.8% of all incidents, but nearly 1 in 4 of them became a notifiable breach. So while third-party incidents are rare, they are much more likely to turn into serious compliance events.
- 4

Operational Speed Is Increasing

Response timelines improved significantly in 2025, with the median discovery-to-notification time reduced by 83 hours. These gains reflect more streamlined downstream processes and stronger operational execution once incidents are identified.

CONTENTS

1. INTRODUCTION	
2. A WORD FROM LEADERSHIP	2
3. DATA BREACH ORIGINS	4
4. DATA BREACH COMPLEXITY	7
5. BREACH RESOLUTION TIMELINES	9
6. FUTURE OF AI IN PRIVACY (BONUS CHAPTER)	11
7. BUILDING DEFENSIBLE AND EFFICIENT PRIVACY PROGRAM	12

DATA BREACH ORIGINS

Understanding where privacy incidents originate is foundational to effective incident management. As response timelines improve and regulatory expectations rise, privacy teams are increasingly challenged not by identifying incidents but by determining which incidents carry meaningful risk and require action.

This chapter examines how incident volume is changing across industries, using anonymized, aggregated metadata from Radar Privacy™. In addition to overall trends, it explores incident sources, such as electronic, paper, and verbal or visual disclosures, along with third-party breach rates and industry-specific patterns. Together, these insights highlight how expanding definitions, regulatory pressure, and operational scale are reshaping the privacy risk landscape and raising the stakes for consistent, defensible decision-making.

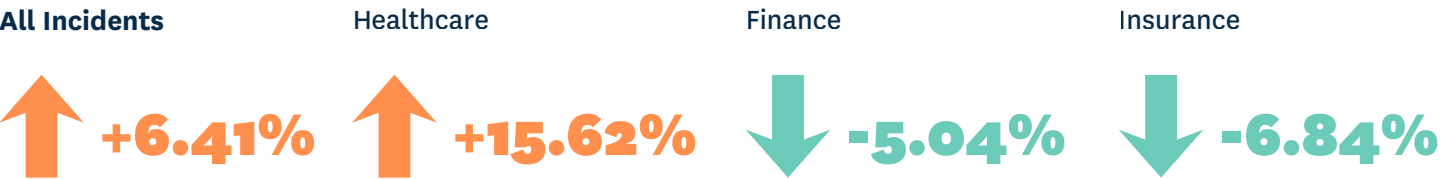
The State of Incident Volume

Overall reported incidents increased 6.41% year over year among organizations that have been using Radar Privacy consistently for at least two years. This makes the increase especially meaningful: it reflects a real rise in reported incidents within a stable customer base, not growth driven by new customers or onboarding effects. As definitions broaden and regulatory expectations rise, incident reporting is becoming more common, expanding the reporting surface rather than simply signaling more attacks.

KEY TERMS

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

Incident volume YoY (2024 vs. 2025)



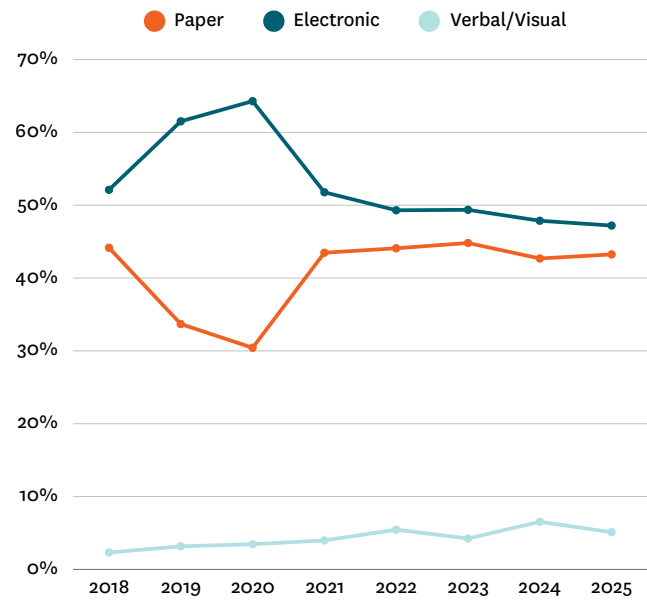
Healthcare shows a clear upward trend in reported incidents compared to financial services and insurance, indicating higher privacy risk in that vertical due to interconnected systems, sensitive data, and regulatory scrutiny.

Incident Source: Where Breaches Begin

The distribution of incident sources remained relatively stable in 2025, reinforcing that growth is being driven by overall volume rather than a shift toward a single incident type. Paper-based incidents increased slightly to 43.25% of total volume, while electronic incidents dipped marginally to 47.21%. Verbal and visual incidents showed the most notable change, falling to 5.11% of incidents as counts dropped by 12.9%, reversing the spike observed in the prior year.

These patterns suggest that privacy risk continues to span multiple channels, underscoring the need for consistent intake and assessment across all incident types.

Incident source: All Industries



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.

Electronic Incident

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

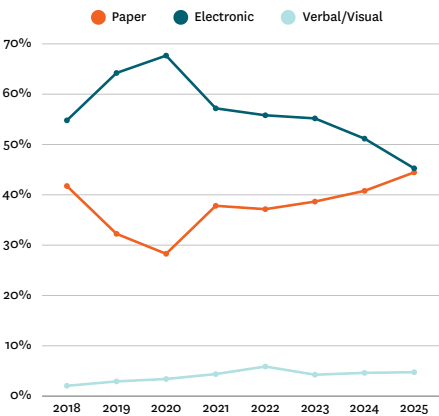
Paper Incident

An unauthorized disclosure of personal information via printed documents.

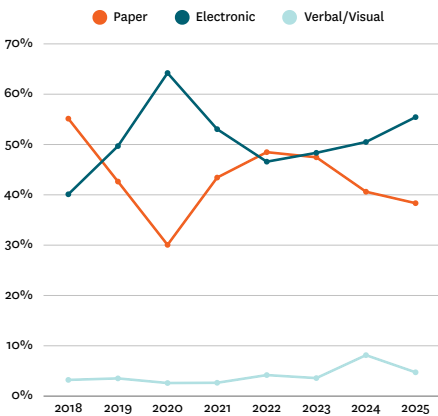
Verbal/visual Incident

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

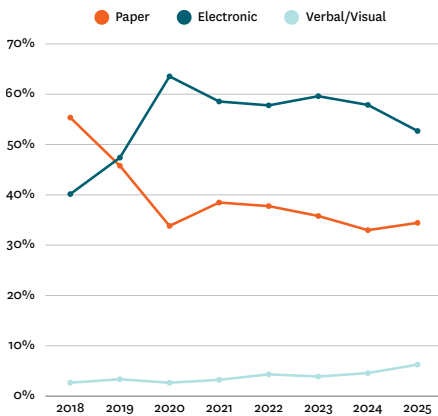
Incident source: Healthcare



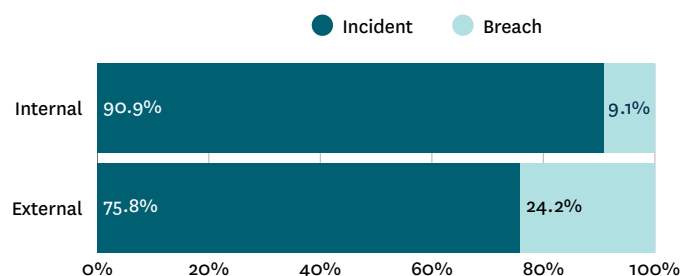
Incident source: Finance



Incident source: Insurance



Breach Rate: Internal vs. External



Third-Party Breach Rate

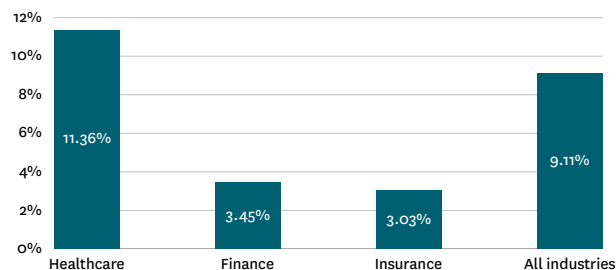
External incidents dropped in frequency (share fell to 4.8%), but the risk of a breach when they do occur jumped to 24.2% (up from 15.9%). Contrast with the Internal Breach Rate (9.1%), reinforcing that third-party risks are "low volume, high severity".

Incident Source by Industry

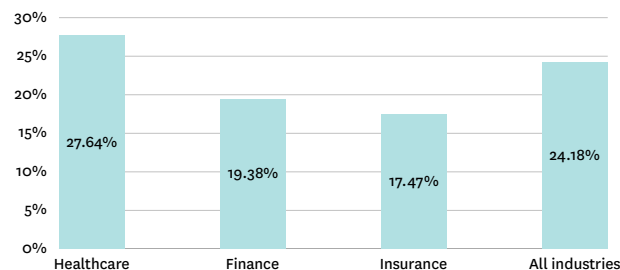
Incident sources vary meaningfully by industry, with healthcare reporting a significantly higher share of internal incidents compared to financial services and insurance. In healthcare, internal incidents account for the vast majority of reported activity, with an **internal breach rate of 11.36%**, while external incidents, though fewer, result in a breach **27.64%** of the time, nearly **2.5× higher** than internal cases.

The contrast is even more pronounced in financial services and insurance. In finance, internal incidents convert to breaches at just **3.45%**, while **external incidents rise to 19.38%**, almost **6× higher**. Insurance shows a similar pattern, with internal breaches at **3.03%** versus **17.47%** for external incidents, again nearly **6× higher**.

Breach Rate: Source Internal



Breach Rate: Source External



These patterns highlight two distinct realities. Healthcare faces a heavier internal operational burden, likely driven by complex workflows and distributed workforces. In contrast, financial services and insurance exhibit stronger internal controls but significantly higher relative risk when incidents originate externally. Across industries, third-party incidents remain less frequent but materially more severe when they occur, reinforcing the importance of vendor oversight and consistent assessment standards.

DATA BREACH COMPLEXITY

As incident volume grows, complexity, more than the frequency, is becoming the defining challenge for privacy teams. Incidents are escalating more quickly, involve more variables, and require more disciplined judgment under increasingly strict regulatory timelines.

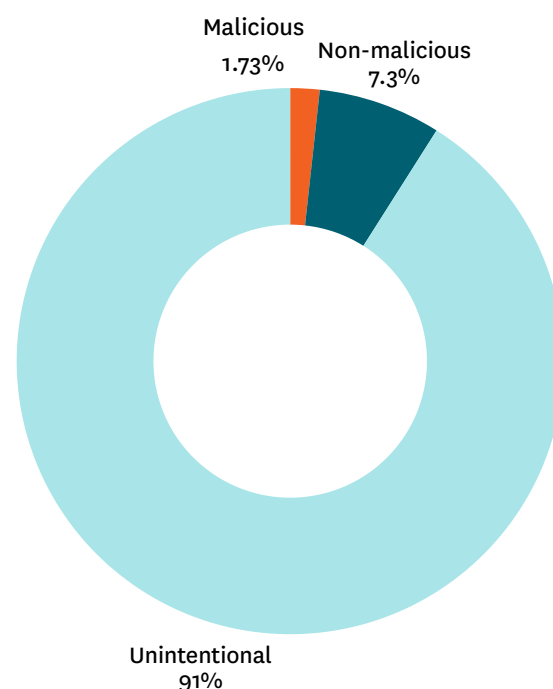
Understanding the intent behind an incident and the scope of exposure is critical to assessing risk and determining appropriate response. This chapter examines the drivers of breach complexity through two lenses: incident intent and scope of exposure. Together, these factors help explain why even seemingly small incidents can carry significant regulatory and reputational consequences, and why consistent, defensible assessment remains essential as privacy teams operate at scale.

Breach Intent

Malicious events continue to represent a small share of overall incidents, accounting for just 1.73% of reported activity. However, despite their low frequency, they are the fastest-growing segment of incidents by intent. In 2025, **malicious incidents increased by 10.3%**, nearly double the growth rate of overall intent-tagged incidents, which rose 5.3%. This gap serves as an important directional risk signal. Human error remains the primary driver of incident volume, but malicious activity is accelerating at a faster pace.

While these incidents occur less often, they tend to escalate more quickly and carry higher regulatory and reputational stakes. The risk profile is therefore shifting from one defined by quantity to one shaped by impact, reinforcing the need for consistent, defensible assessment as incident intent becomes more consequential over time.

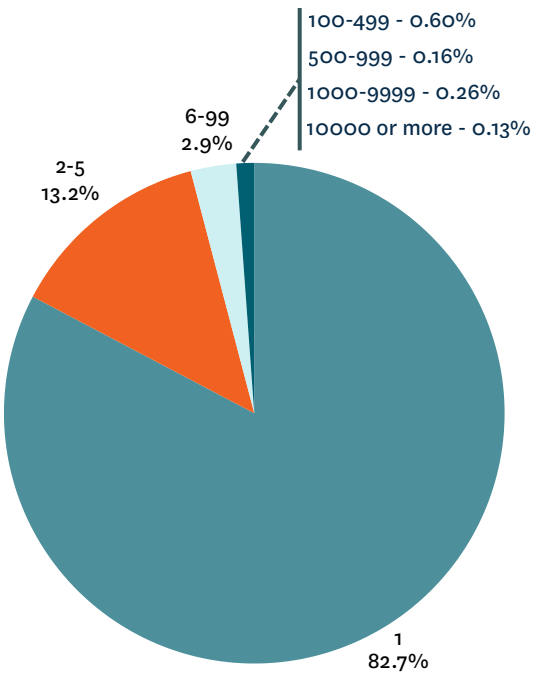
Breach Intent



Scope of Exposure

The scope of exposure per incident widened in 2025. The average number of individuals impacted per assessed incident rose from 345 to 830 individuals (an increase of 140%). However, this change was driven primarily by a small number of very large-scale incidents involving substantial populations, rather than a uniform shift in incident severity across the board.

Individuals Impacted per Incident



Despite the higher overall average, 96% of incidents in 2025 still involved five or fewer individuals.

This reinforces the need for consistent assessment across all incident types. While major events draw immediate attention, sustained operational and regulatory risk is driven by the steady volume of smaller cases. Organizations cannot afford to overlook smaller incidents simply because they affect fewer individuals, as handling them carefully and documenting decisions helps maintain compliance and prevents recurring issues from turning into larger problems.

82.71%

The share of “1-person” incidents increased by 1.3% point from 2025 and reached 82.71%.

Jurisdictional Complexity

Jurisdictional complexity declined modestly in 2025, with the average number of jurisdictions per breach decreasing from 3.00 to 2.65. More notably, the distinction between breaches and non-breaches continued to narrow. Historically, incidents requiring notification clearly involved a greater number of jurisdictions than non-reportable incidents. However, that gap has contracted, with the difference in average jurisdiction counts declining from 1.73 to 1.35 between 2024 and 2025.

This convergence suggests that the number of jurisdictions involved is becoming a less reliable differentiator between incidents that trigger notification obligations and those that do not. While multi-jurisdictional exposure remains an important compliance consideration, jurisdictional spread alone is no longer as strong an indicator of breach severity or regulatory impact as it has been in prior years.

BREACH RESOLUTION TIMELINES

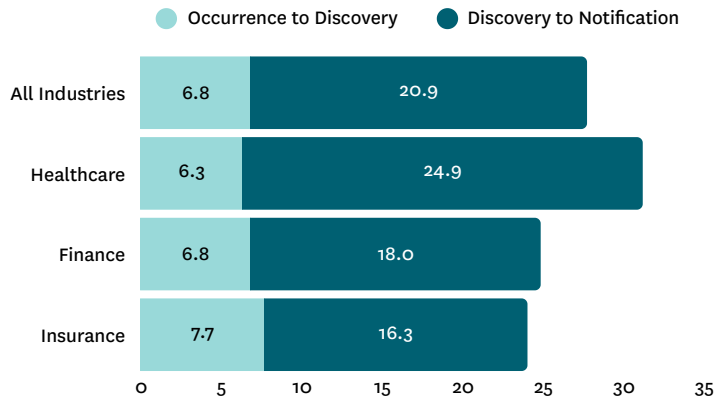
Accelerating Resolution

Breach resolution timelines represent one of the clearest areas of progress in this year’s report. Discovery-to-Notification time declined by 82.8 hours (3.5 days), **bringing the average down to 501.9 hours (20.9 days)**, while Discovery-to-Assessment improved by 63.8 hours (2.7 days). These gains reflect sustained investment in process maturity and tooling. Notably, this significantly outpaces broader benchmarks, in 2022 [Gartner reported](#) organizations took an average of 79.8 days to report incidents to regulators (up from 60.6 days in 2020), compared to just 20.9 days for Radar Privacy users last year.

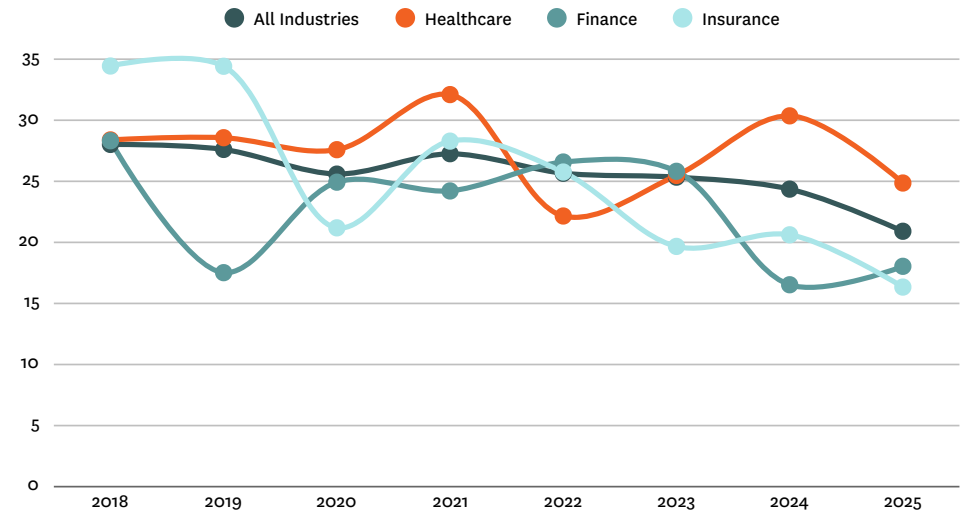
20.9 days

Organizations using Radar Privacy™ average just 20.9 days to discover, assess, and issue breach notifications.

Timeline: Occurrence to Discovery + Discovery to Notification



Timeline: Discovery to Notification



KEY TERMS

Occurrence Date
The date an incident took place.

Discovery Date
The date an organization became aware of an incident.

Notification Date
The date of required notification to regulators or individuals or contractual obligations to clients.

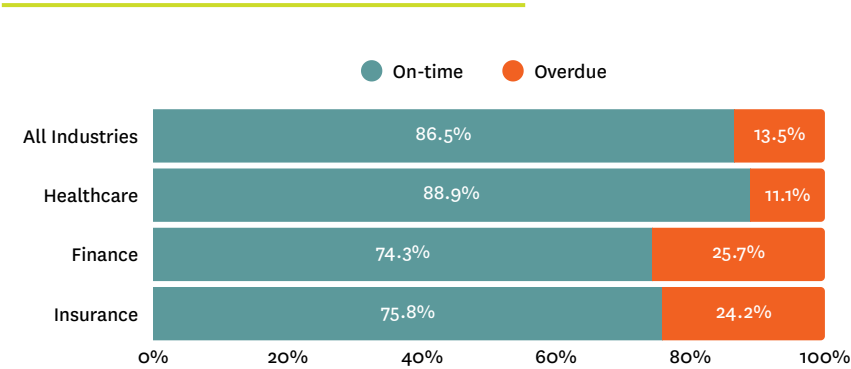
On-Time Performance (Overdue Notification)

Organizations continued to make meaningful progress in meeting breach notification deadlines in 2025. Overall **overdue notifications declined to 13.53%**, representing a 3.74 % point improvement from the prior year. This reduction reflects stronger operational discipline and more consistent execution once notification obligations are identified.

However, performance varies significantly by industry. Healthcare continues to lead, with overdue notifications at 11.10%, setting a benchmark for timely response. In contrast, financial services (25.72%) and insurance (24.19%) continue to experience materially higher overdue rates. Despite overall improvements, these industries remain nearly twice as likely as healthcare organizations to miss a notification deadline.

Part of this gap likely reflects differences in regulatory timelines. Financial services and insurance often face shorter reporting windows, sometimes as little as 72 hours, while healthcare laws typically allow 30 to 45 days. These compressed deadlines increase execution pressure and make on-time performance more challenging.

On-Time Notification v. Industry



These gaps underscore that while on-time performance is improving overall, industry context and operational complexity continue to influence outcomes. Closing the remaining gap will require continued focus on standardized workflows, clear escalation paths, and consistent execution under regulatory timelines.

Compliance Precision

The percentage of **incidents requiring notification increased to 9.84%** across all industries, up 1.25 % points from the prior year. Healthcare continues to stand out, with a higher notifiable rate than financial services and insurance, which remain comparatively low. This increase is likely driven by regulatory changes and stricter enforcement rather than a shift in the types of incidents organizations are experiencing.

Notifiable incidents

Healthcare **12.03%** Finance **4.17%** Insurance **3.91%**

BONUS CHAPTER

FUTURE OF AI IN PRIVACY

What happens when the same technology that accelerates efficiency also amplifies privacy risk?

New tools are rapidly reshaping privacy operations, creating both meaningful gains and new categories of exposure. AI presents both an opportunity for increasing operational efficiency and a growing threat to privacy. In 2025, that tension became increasingly visible in real-world incident data.

The [2025 Stanford AI Index Report](#) found that AI-related privacy and security incidents increased by approximately 56% year over year, underscoring how quickly AI-driven risks are emerging. These incidents often differ from traditional privacy events, involving automated decision-making, large-scale data ingestion, or novel attack vectors, and therefore require more specialized tracking and assessment.

“By 2027 AI governance will be required under the sovereign AI regulations worldwide and organizations that cannot integrate governance will face competitive disadvantage”

Source: Gartner

The growing use of AI has also accelerated the sophistication and scale of social engineering attacks. Tools capable of generating highly realistic phishing messages and voice deepfakes have expanded the risk of impersonation and fraud. According to [Security Today](#), 82.6% of phishing emails analyzed between September 15, 2024, and February 14, 2025 contained some use of AI, highlighting how deeply AI is now embedded in common threat patterns.

+56%

AI-related privacy and security incidents increased by approximately 56% year over year.

Together, these trends point to a clear need to manage AI-related incidents as a distinct category of operational and regulatory risk. Treating them as traditional privacy events risks obscuring their root causes, accountability structures, and broader impact. At RadarFirst, we see the future of AI and privacy not as separate conversations, but as an evolution of incident discipline itself. As AI systems introduce new forms of risk, organizations will need structured processes that determine notification obligations, clarify accountability, and produce defensible documentation consistently, and at scale.

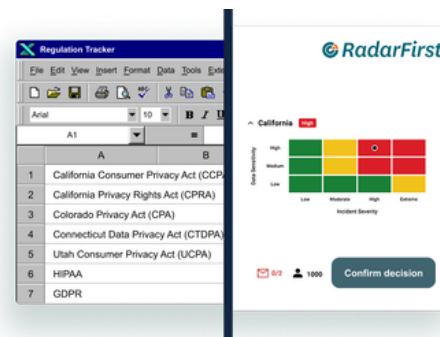
BUILDING DEFENSIBLE AND EFFICIENT PRIVACY PROGRAM

This year's findings reinforce a clear conclusion: privacy incident management has entered a faster, higher-stakes era. Incident volume continues to rise, malicious risk is accelerating, and third-party and electronic incidents carry an outsized impact when they occur. While organizations have made real progress in improving response speed and meeting notification deadlines, risk is no longer defined by volume alone; it is shaped by impact, intent, and execution under pressure. In this environment, defensibility and efficiency are inseparable.

By operationalizing incident response with platforms like Radar Privacy™, organizations can bring clarity and consistency to complex regulatory decisions. As privacy risk evolves, teams that prioritize precision and agility in incident management will be best positioned to ensure compliance and protect trust.

The Rise of the Defensible Decision

Privacy incident management is entering a new governance era. Regulators, proxy advisors, and boards are placing greater scrutiny not only on how organizations respond to incidents, but on how critical decisions are made under pressure. Materiality determinations, notification judgments, and risk assessments now carry consequences that extend beyond regulatory compliance, influencing investor confidence, legal exposure, and corporate reputation.



As a result, execution alone is no longer sufficient. Organizations must be prepared to demonstrate that decisions were made reasonably, consistently, and with clear rationale. This shift marks an important evolution in operational maturity. Speed remains essential, but defensibility is emerging as the defining capability of modern incident management. The ability to operationalize judgment, applying structured, repeatable decision-making across incidents, is becoming as critical as the response itself.

ORGANIZATIONS MUST BE PREPARED TO DEMONSTRATE THAT DECISIONS WERE MADE REASONABLY, CONSISTENTLY, AND WITH CLEAR RATIONALE.

The data in this report reflects that transformation. Improvements in response timelines signal growing operational discipline, while rising incident complexity reinforces the need for consistent evaluation under increasing scrutiny. Risk is no longer defined solely by the incident. It is defined by the decision that follows.

Running the Uphill Sprint with Confidence



Consistency over perfection

Defensibility does not come from perfect decisions; it comes from applying the same decision-making process every time. Regulators and auditors look for reasonable, consistent judgment, not flawless outcomes. Programs that rely on ad-hoc interpretation introduce unnecessary risk when incident volume increases.



Repeatable response workflows

Repeatable workflows reduce dependence on individual judgment during high-pressure incidents. When response steps are standardized, teams can move faster without sacrificing accuracy, even as incident volume and complexity grow.



Standardized intake and classification

Clear intake and classification processes allow incidents to be triaged quickly and consistently. Standardization ensures that similar incidents are handled the same way, reducing delays, rework, and confusion across teams.



Documented decisions

Documented decisions are critical to defensibility. Clear records demonstrate that assessments were made thoughtfully, within required timelines, and based on available information at the time, providing essential protection if decisions are questioned later.



Centralized visibility and ownership

Centralized visibility creates accountability. When ownership, status, and decisions are visible across privacy, legal, security, and compliance teams, organizations reduce blind spots and ensure incidents do not stall or escalate unnoticed.



Built to scale and adapt

Privacy programs must be designed for growth and change. Regulatory requirements evolve, incident volume fluctuates, and new risk patterns emerge. Programs built to scale can absorb these shifts without breaking, maintaining consistent performance even during spikes or periods of disruption.

The uphill sprint is not slowing down. The pace is faster, the terrain is steeper, and the stakes are higher. Organizations that invest in consistent, efficient, and defensible privacy incident management are best positioned to meet these demands; not just to respond, but to operate with confidence in an increasingly unforgiving risk environment.

ABOUT RADARFIRST

RadarFirst is an AI-forward regulatory risk management platform for privacy and AI governance. Trusted by leading organizations, RadarFirst enables teams to manage incidents with speed, consistency, and defensibility by standardizing how incidents are captured, assessed, and actioned.

With more than a decade of experience supporting real-world privacy incidents, including more than 1 million incidents managed, 4 million regulatory decisions delivered, and more than \$2 trillion in revenue protected, RadarFirst brings proven discipline to modern regulatory risk. As AI drives greater incident volume, complexity, and scrutiny, RadarFirst helps organizations prepare before risk becomes operational.

\$2 Trillion

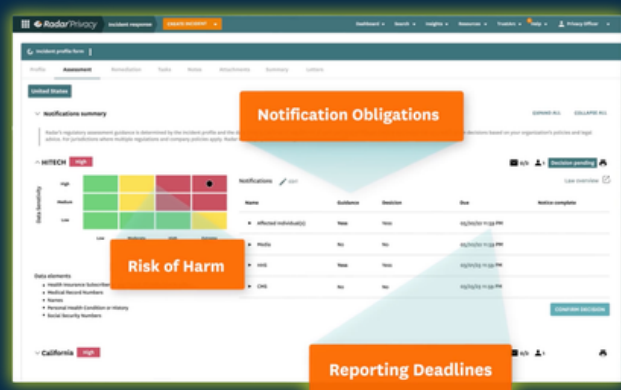
CLIENT REVENUE
PROTECTED

0

SPREADSHEETS
REQUIRED

98%

CUSTOMER
RETENTION



**WANT TO SEE
RADARFIRST IN ACTION?**

SCHEDULE DEMO TODAY



