RadarFirst

2025 Privacy Incident Management Benchmarking Report

Data to Operationalize Compliance and Increase Resilience from Data Breaches

A word from leadership

Privacy incidents are no longer rare events—they are an operational certainty. As organizations collect and process more data than ever, privacy and compliance teams face increasing complexity in managing risk, navigating regulations, and maintaining public trust. The challenge is no longer just about securing data but ensuring the right governance, response, and risk assessment strategies are in place to mitigate potential harm.

Compounding this challenge is the rapid proliferation of artificial intelligence. AI is transforming how organizations operate, offering automation, efficiency, and powerful data-driven insights. But with AI growth comes heightened privacy risks to sensitive data being ingested at scale and new regulatory frameworks emerging to oversee its use. As AI evolves, regulatory oversight and governance will grow at an unprecedented pace. Privacy and compliance teams must evolve alongside these innovations, ensuring that AI-driven processes remain transparent, compliant, and defensible under board or regulatory scrutiny.

At RadarFirst, we believe that strong privacy governance isn't just about compliance—it's about resilience. Our work with leading organizations has shown that teams who invest in automation, precision, and proactive risk management are best positioned to reduce breach resolution times, limit risk exposure, and build lasting trust. The 2025 Privacy Incident Benchmarking Report is a testament to these evolving challenges and the solutions organizations require to succeed.

This year's findings underscore critical truths: human error continues to drive the majority of privacy incidents, third-party risks are escalating, and regulatory complexity is making precision in incident response more important than ever. Organizations that rely on manual, reactive processes are struggling to keep pace, while those leveraging automation and risk-based decision-making are mitigating risks more effectively and ensuring compliance with speed and confidence.

The insights in this report serve as both a benchmark and a guide for privacy teams navigating the future. The landscape is changing, and the organizations that act now—by strengthening governance, leveraging technology, and prioritizing resilience—will set the standard for data responsibility in the years ahead.

Sincerely,

Zach Burnett
CEO, RadarFirst

As privacy professionals, we know that compliance isn't just a box to check, it's a commitment towards trust, accountability, and resilience. In an era where data breaches dominate headlines and regulations shift faster than ever, privacy teams face unprecedented pressure to respond swiftly and accurately to incidents.

Every year, the Privacy Incident Benchmarking Report provides a critical snapshot of the challenges and opportunities shaping our industry. Organizations that invest in scalable, automated incident response workflows are seeing real, quantifiable results — reducing breach resolution times and improving compliance outcomes. Radar Privacy users, for example, have cut the time from incident discovery to resolution nearly in half compared to their industry peers.

This report is designed for privacy leaders, legal teams, security professionals, and executives who recognize that proactive privacy management is a competitive advantage. It serves as both a benchmark for industry performance and a strategic guide to navigating the evolving landscape of regulatory risk.

At RadarFirst, accuracy matters. The right technology, policies, and training empower privacy teams to make faster, smarter, and more defensible decisions, protecting organizational compliance and consumer confidence.

I encourage you to explore these insights, reflect on your own organization's approach, and consider what steps you can take today to build a more resilient privacy program for the future.

Sincerely,

Lauren Wallace
General Counsel & Chief Privacy Officer, RadarFirst

Executive Summary

1 **Third-Party Risk is a Growing Concern**

Incidents from third parties are nearly twice as likely to require notification. According to Gartner, 45% of organizations will have experienced attacks on their software supply chains in 2025, emphasizing the need for stronger vendor risk management.

2 **Human Error is the Leading Cause of Breaches**

91.3% of breaches stem from non-malicious errors. A significant 81.7% of incidents involve a single individual, showing that everyday errors—not cyberattacks—are the primary concern.

3 **Compliance Complexity is Increasing**

Overlapping regulations demand precise notification timelines. Automation and cross-jurisdictional compliance strategies are essential for minimizing legal exposure and avoiding reporting delays.

4 **Faster Breach Resolution is a Competitive Advantage**

Time-to-resolution improved from 24.3 days (2018) to 14.6 days (2024). Organizations using automated risk assessment tools dramatically reduce financial and reputational risks.

5 **Precision in Breach Notification Prevents Compliance Pitfalls**

With automation, organizations achieve 83.7% on-time notifications. Over-reporting wastes resources and may trigger needless regulatory scrutiny and a decline in customer trust; under-reporting can lead to regulatory fines and reputational harm. Automating risk assessments with Radar Privacy reduces the risk of both.

6 **Privacy Awareness Strengthens Security Culture**

Privacy breaches aren't just digital—paper and verbal disclosures matter too. Comprehensive privacy training helps organizations prevent non-technical breaches and build resilience.

CONTENTS

Data Breach Origins

Data breaches are an inevitable and costly reality of doing business in today's digital climate. Regulators across the globe recognize this and expect organizations to be well-prepared for such incidents by building robust incident response and disaster preparedness procedures as integral parts of their data collection and risk management strategies.

At RadarFirst, we understand the critical importance of being prepared, and our 2025 Privacy Incident Management Benchmarking Report is proof of our commitment to helping organizations navigate these challenges effectively.

By leveraging the insights and best practices presented in this report, organizations can better prepare for and respond to privacy incidents, ensuring they meet regulatory requirements and maintain the trust of their stakeholders.

The data featured in this report is derived from anonymized and aggregated Radar Privacy metadata to ensure the protection of our customers' privacy and confidentiality.

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.

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

Internal Incident
An incident that originates within an organization due to intentional or unintentional employee action.

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

Third-Party Breach Rate

The risk of third-party breaches has become a critical concern for organizations worldwide. Gartner predicts that in 2025, a staggering **45% of global organizations will have fallen victim to a software supply chain attack**, highlighting the growing vulnerability of even the most robust security frameworks. This alarming statistic underscores the urgent need for organizations to reassess their third-party risk management strategies. Compounding this issue, a recent study by Prevalent reveals that **61% of companies have already experienced a breach originating from a third party.**

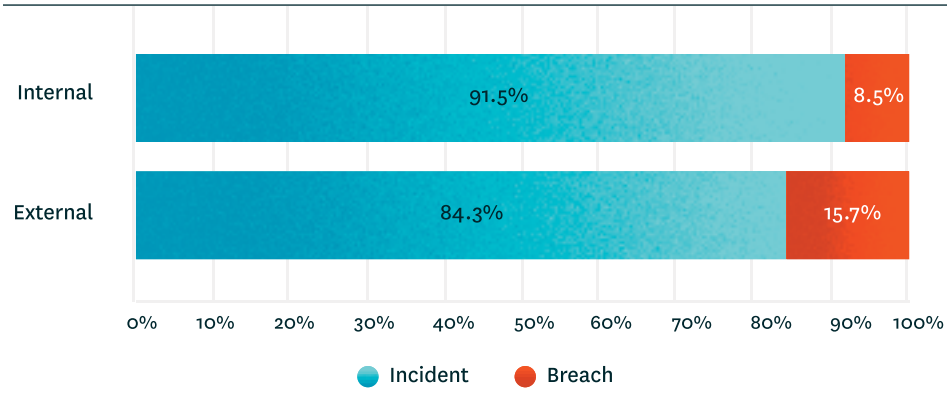
Our metadata further emphasizes this trend: **incidents stemming from third-party vendors are almost twice as likely to result in a notifiable breach.** This section delves into the complexities and implications of third-party breach rates, offering insights and actionable recommendations to mitigate these risks and protect sensitive information.

45%

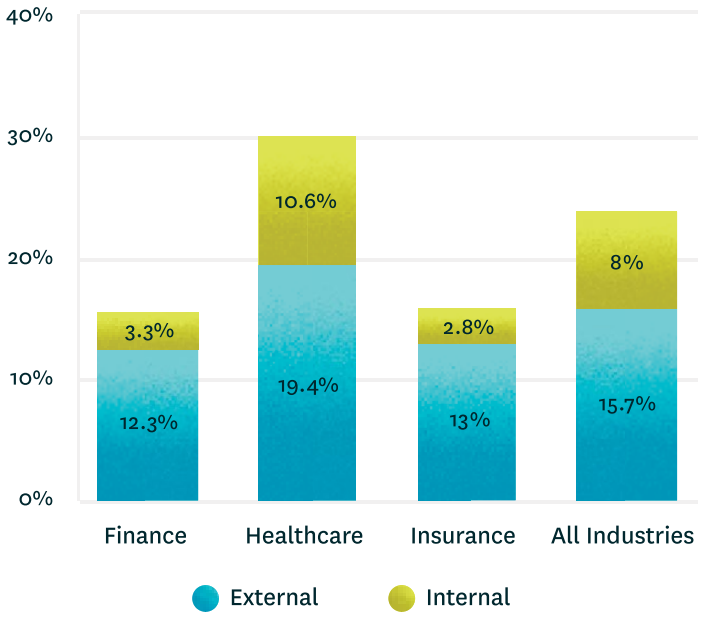
By 2025, a staggering 45% of global organizations will have been the victim of a software supply chain attack.

— Gartner

Breach Rate: Internal v. External



Incident Source v. Industry



Incident Source by Industry

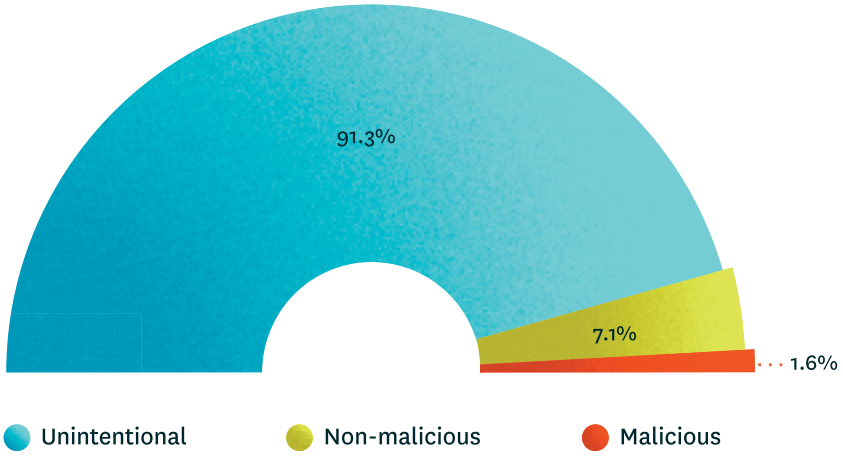
Third-party vendor relationships vary significantly across industries, each with unique risks. In healthcare, vendors handling patient data can lead to severe privacy breaches. Financial services face significant financial and reputational risks from third-party functions like payment processing and mailing services. Insurance companies, relying on third parties for data analytics, risk compromising customer data and undermining risk assessments. **Regardless of the industry, tailored risk management strategies are essential to address third-party risks effectively.**

How a Fortune 50 Health Insurer Manages Hundreds of Incidents Every Quarter

Breach Intent

For many organizations, creating urgency around privacy awareness and training only happens after a significant breach. For Boardroom and C-suite decision-makers, the daily operational risks of data breaches don't come into focus until the media is involved. However, according to Radar Privacy metadata, **the vast majority of data breaches are not the result of outside threats or cyberattacks from malicious actors but, rather, routine errors stemming from human oversight.**

Breach Intent



While less threatening on the surface, these incidents require the same level of scrutiny and attention to detail that large breaches involve, and include the same requirements for risk assessment and limited notification timelines as large breaches.

A mature privacy program can intake, triage, assess, and document 100% of the incidents that are reported before making notification decisions. In aggregate, **Radar Privacy users report only 8.5% of all incidents** (in some industries, the notification rates are significantly lower).

To meet compliance with new and changing regulations, organizations must instill proactive privacy measures that equip employees with the knowledge and skills to report incidents when they occur to reduce risk organization-wide.

8.5%

Radar Privacy users report only 8.5% of all assessed incidents.

Would Your Team Be Ready If This Happened Today?

Run a Privacy Tabletop Exercise with your team using a real-world scenario. Practice before a breach hits.

Run the Exercise

Breach Complexity

No two breaches are alike. Understanding the specific nature of an incident's origin can be instrumental in developing effective strategies to prevent similar occurrences in the future.

However, organizations face a growing number of challenges when responding to privacy incidents. The privacy landscape is **increasingly complex**, with new laws and regulations emerging regularly, often with overlapping and nuanced requirements. These laws also frequently have unique timelines for reporting and responding to incidents, making compliance difficult. Additionally, privacy teams are often **understaffed and under-resourced**, struggling to keep up with the demands of incident response, especially when dealing with multiple incidents simultaneously.

By carefully analyzing the root causes of past incidents and implementing targeted preventative measures, organizations can significantly reduce their risk of future data breaches and protect sensitive information.

University Medical Center Relies on Radar® Privacy for Compliance with HIPAA and U.S. State Data Breach Laws

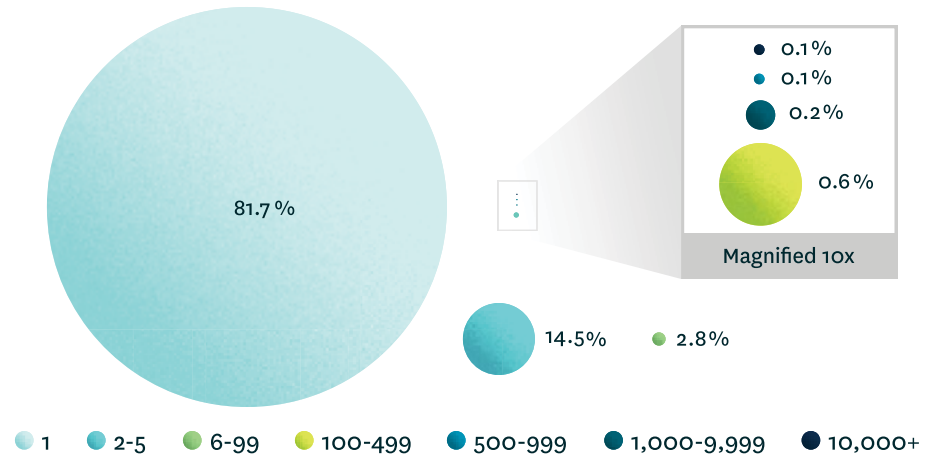
KEY TERMS

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.

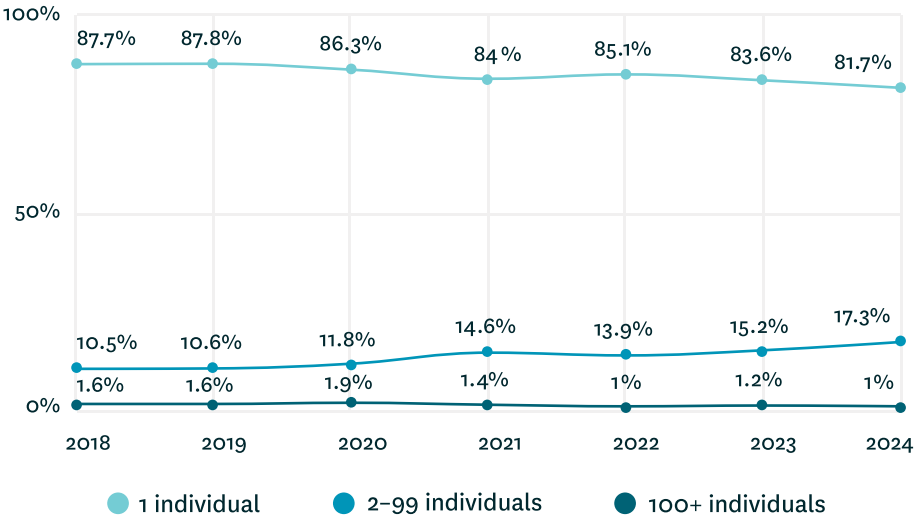
Individuals Impacted per Incident



Scope of Exposure: Trends in Affected 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 requirements to be compliant.

Percentage Change: Small v. Large Incidents



Minor Incidents and Major Problems

Although more complex to untangle, large incidents account for less than 2% of all assessed incidents, historically. The work that keeps privacy teams busy is often the assessment and notification decision-making around small incidents that impact only one individual. Since 2018, the number of single-person incidents that require assessment from a privacy professional has occupied **more than 81% of all required work.**

In the long run, does your organization spend more time assessing complex incidents or simple incidents?

Breach Resolution Timelines

In the world of data privacy, time is money. The moment a privacy incident is discovered, the regulatory clock starts ticking, and with it, the risk of hefty penalties and the immeasurable loss of customer trust. To maintain compliance and uphold public confidence, organizations must act quickly to assess incidents, determine notification obligations, and inform affected individuals, business partners, and regulatory authorities.

The window between **incident discovery and notification** is a critical period where advanced privacy incident management solutions set mature organizations apart. **Automation, structured workflows, and real-time risk assessments** can dramatically reduce response times and improve compliance outcomes.

Organizations using Radar Privacy **average just 31.6 days** to discover, assess, and issue breach notifications.

To strengthen **organizational resilience**, businesses must critically evaluate their **breach response timelines**. Ensuring compliance with legal mandates while proactively mitigating the impact of data breaches requires a strategic approach—one that prioritizes speed, efficiency, and transparency in incident resolution.

31.6 days

Organizations using Radar Privacy average just **31.6 days** to discover, assess, and issue breach notifications.

KEY TERMS

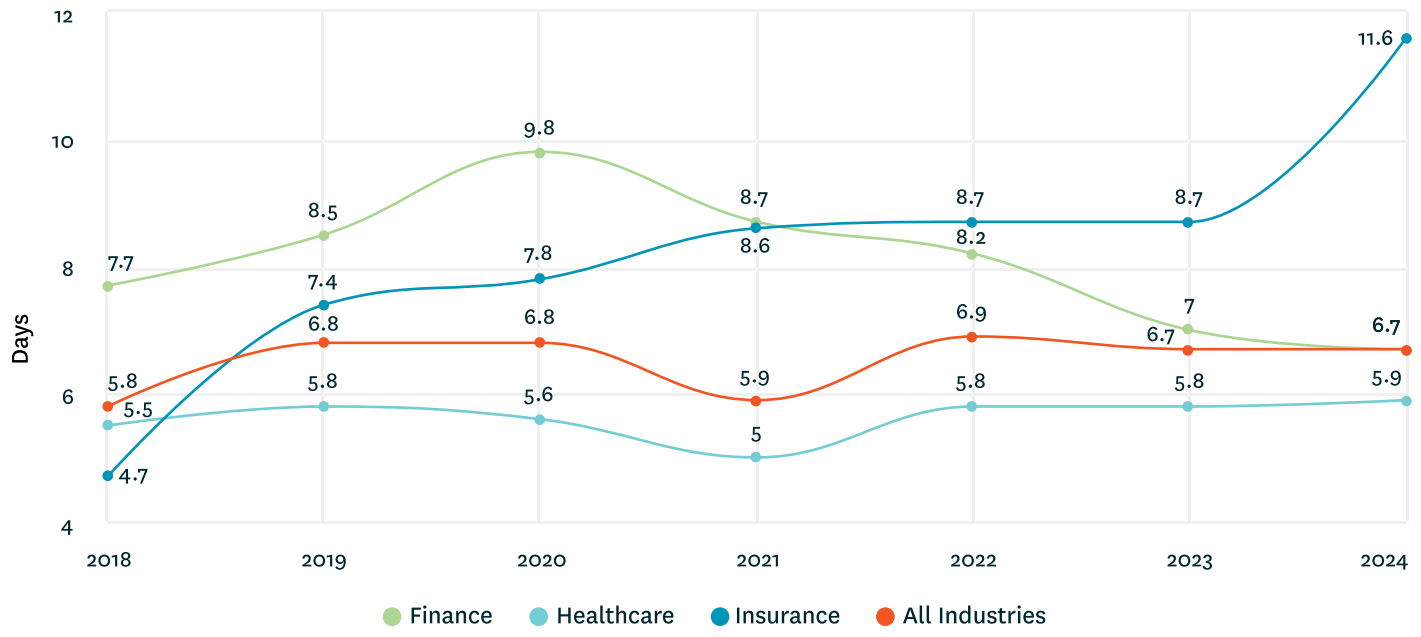
Occurrence Date
The date an incident took place.

Discovery Date
The date an organization became aware of an incident involving personal information.

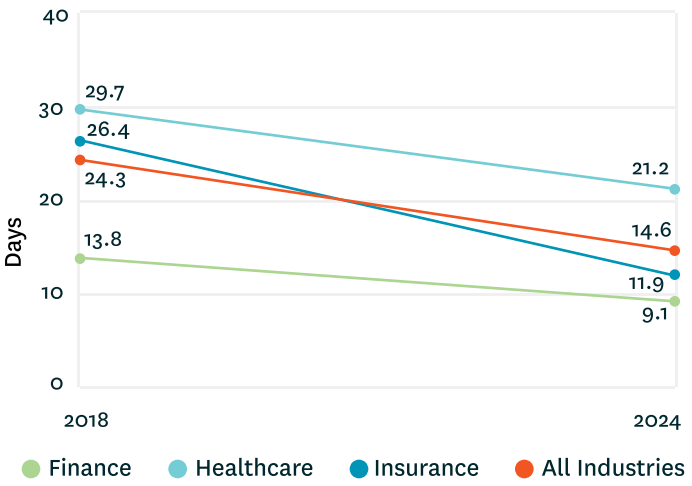
Notification Date
The date of required notification to regulators or individuals (e.g., within 72 hours or 30 days) or contractual obligations to clients (which often have much shorter notification windows).

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

Timeline: Occurrence to Discovery



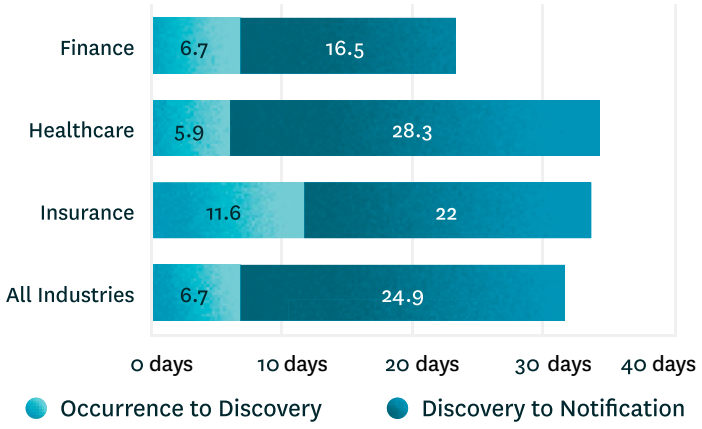
Timeline: Discovery to Assessment



9.7 days

On average, Radar Privacy users have reduced the time from the discovery of an incident to risk assessment by 9.7 days since 2018.

Timeline: Occurrence to Discovery + Discovery to Notification



What Would It Look Like to Cut Notification Timelines by 40%?

See how Radar Privacy streamlines your risk assessments and notification workflows.

Schedule a Demo

On-Time Notifications: Balancing Speed and Accuracy

Timely and accurate breach notification is a critical measure of an organization's privacy program maturity. While regulatory deadlines dictate when notifications must be made, the ability to conduct **a risk assessment** before reporting is what distinguishes proactive, well-equipped organizations from those forced into blanket reporting.

83.7%

Organizations using Radar Privacy achieve an impressive **83.7% on-time notification rate.**

Our metadata reveals that organizations using **Radar Privacy achieve an impressive 83.7% on-time notification rate**, demonstrating their ability to assess incidents efficiently while meeting legal deadlines. In contrast, organizations without automated privacy incident management solutions often default to notifying on **100% of incidents**, not because all require disclosure, but because they lack the time, capacity, or tools to determine which ones **rise to the level of being notifiable** under jurisdictional law(s).

This indiscriminate reporting strategy can introduce **significant risks**:

Over-reporting

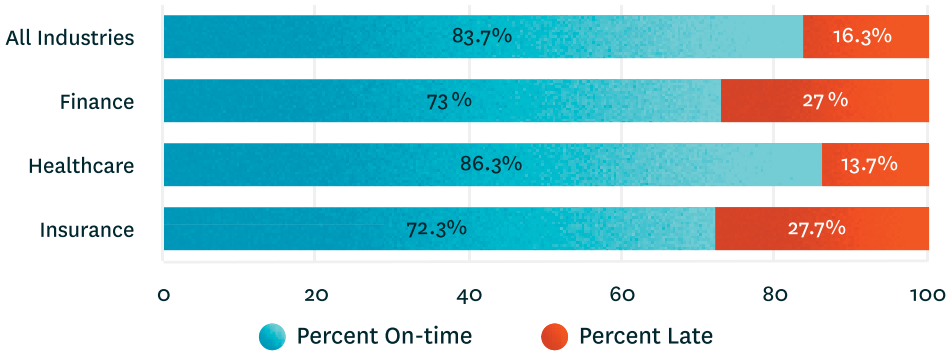
When organizations notify on every incident, even those that pose little to no harm, they risk "**alert fatigue**" among regulators and stakeholders. Repeated, unnecessary breach notifications can damage brand credibility, erode consumer trust, and even invite increased regulatory scrutiny.

Under-reporting

Failing to notify when required can lead to severe **compliance violations, financial penalties, and reputational damage**—not to mention potential litigation and loss of customer confidence.

The key to reputational resilience is precision—ensuring notifications are made only when necessary and always on time. By leveraging automation for privacy incident management, organizations can accurately assess risk, meet legal obligations, and maintain trust without resorting to over-reporting as a default strategy. For audit purposes, all incidents should be documented to ensure compliance for present and future cases.

On-Time Notification v. Industry



Organizations in industries with shorter regulatory notification timelines, such as finance and insurance, often experience a correlation with a higher number of electronic incidents, potentially leading to increased compliance pressures and challenges to meeting regulatory reporting timelines.

Healthcare organizations experience a large amount of cyberthreats and threats to PHI, however the 60-day notification period granted by HIPAA correlates with a higher percentage of on-time notifications compared to industry peers in finance or insurance.

The Importance of Privacy Awareness in an Evolving Data Breach Landscape

As business practices evolve and technology continues to reshape operations, privacy risks are no longer confined to traditional data breaches. The types of incidents that escalate into reportable breaches are influenced by shifting regulatory landscapes, emerging technologies, and changes in how organizations handle sensitive data.

A strong privacy awareness and incident reporting program is essential for equipping employees with the knowledge to identify, assess, and escalate incidents across all **data formats**, whether **electronic, paper-based, or behavioral**. Without proper training, even well-intentioned employees may overlook risks or fail to recognize when an incident requires further investigation.

Why Privacy Training is Critical for Incident Management

Beyond Digital Breaches

While cybersecurity incidents dominate headlines, **paper-based misdeliveries, verbal disclosures, and improper data handling** remain significant sources of privacy breaches. Employees must be trained to recognize and report all types of incidents, not just those involving electronic systems.

Early Detection Reduces Risk

The sooner an incident is identified, the faster it can be assessed and mitigated. Training employees to recognize suspicious activity, such as unauthorized access, misrouted information, or inappropriate data sharing, helps reduce **both regulatory risk and reputational damage**.

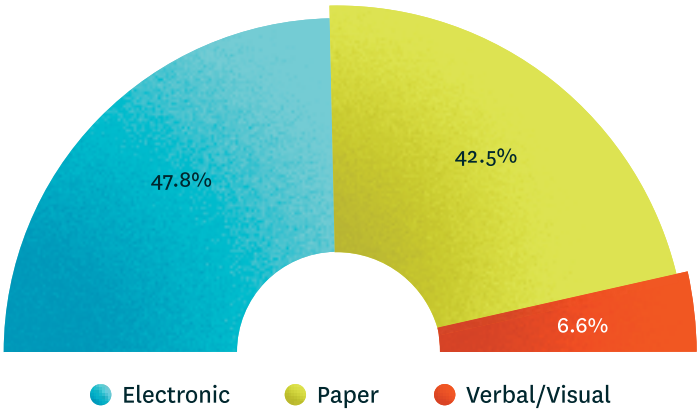
Regulatory Compliance & Due Diligence

Regulations like **GDPR, HIPAA, and CPRA** require organizations to demonstrate due diligence in safeguarding personal data. A well-documented, ongoing privacy training program is not just best practice—it's an essential component of regulatory compliance.

A Culture of Privacy & Trust

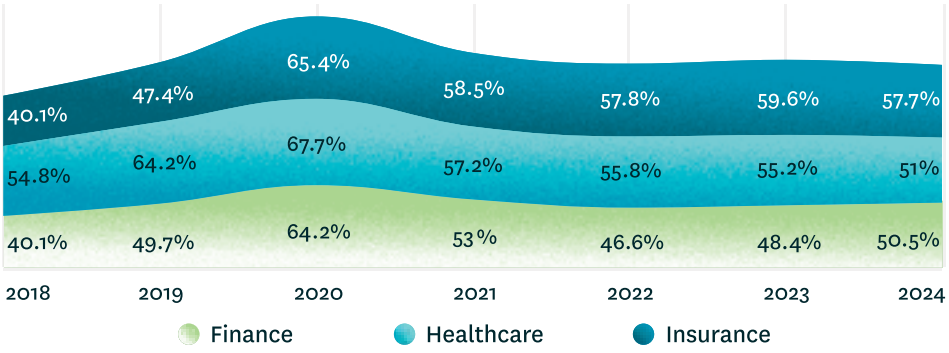
Embedding privacy awareness into daily operations fosters a culture where employees feel empowered to report concerns. This proactive approach **strengthens an organization's overall security posture** and builds long-term trust with customers, partners, and regulators.

Incident source: All Industries

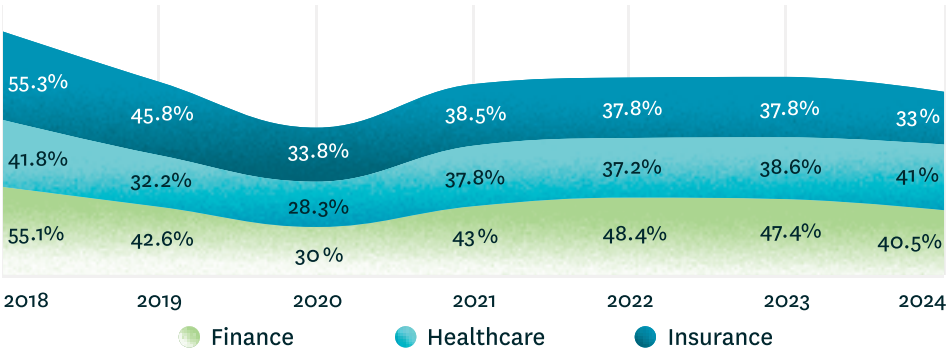


As privacy risks continue to expand beyond traditional cyber threats, **comprehensive privacy training is a strategic necessity**. Organizations that prioritize education across all areas of data handling will be best positioned to minimize breaches, maintain compliance, and uphold public confidence in their privacy programs.

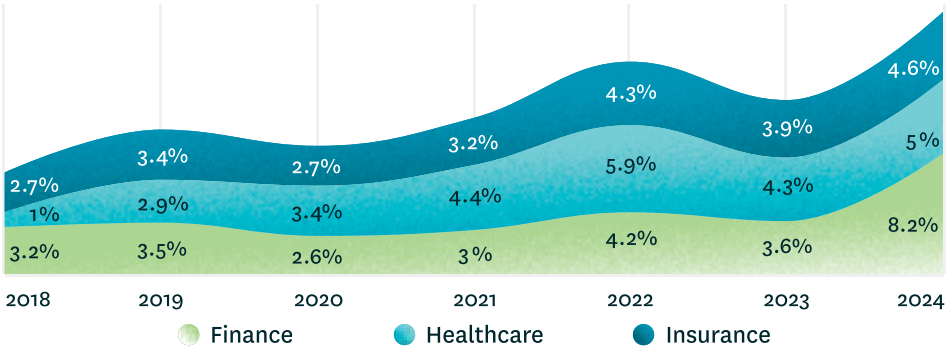
Electronic incidents by industry: 2018–2024



Paper incidents by industry: 2018–2024



Verbal/Visual incidents by industry: 2018–2024



Building Privacy Resilience

This year's findings underscore a critical reality for privacy teams: the complexity of incident management is increasing, driven by evolving regulatory requirements, growing third-party risks, and the persistent challenge of human error.

With third-party vendors playing an expanding role in business operations, organizations must be more vigilant than ever in assessing and mitigating external risks. At the same time, our data reaffirms that **human error remains the leading cause of data breaches**, highlighting the urgent need for **robust privacy training, proactive risk assessments, and streamlined incident response workflows**. These challenges reinforce the importance of precision in breach assessment, ensuring that organizations report what's necessary, on time, and with confidence.

Amidst these complexities, **privacy teams are not alone**. RadarFirst continues to provide cutting-edge solutions that empower organizations to **simplify compliance, reduce risk, and build trust through automation and intelligent decision-making**.

Human error remains the leading cause of data breaches

A Fortune 150 Financial Company Selects Radar® Privacy for Consistent Risk Assessment

By embracing **automated incident response strategies, investing in ongoing education, and leveraging technology to accelerate breach resolution**, organizations can navigate regulatory uncertainty with clarity and confidence. As the privacy landscape evolves, those who prioritize agility and precision in their incident management approach will be best positioned to **protect their customers, ensure compliance, and strengthen their reputational resilience.**

Resources

Privacy Team Tabletop Exercise

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

www.radarfirst.com/privacy-tabletop

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

Radar Privacy Buy-in Guide

You know the importance of privacy incident management to your organization and customers, but now you need to convince your decision makers. This guide will help you build a business case.

www.radarfirst.com/resources/radar-privacy-buy-in-guide

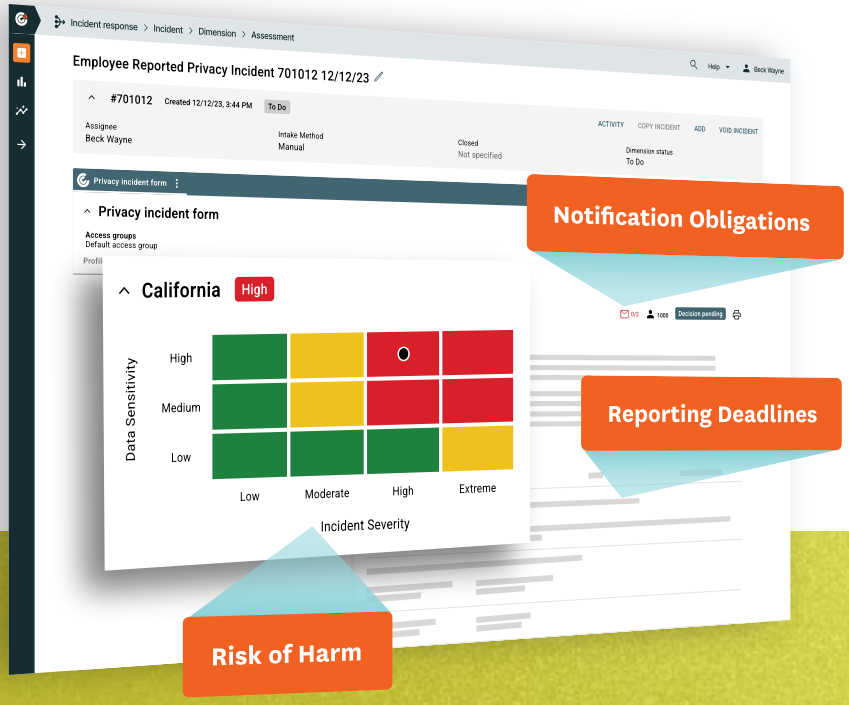
Radar Privacy Demo

Find out why 99% of customers stick with RadarFirst.

www.radarfirst.com/demo-request

SEE RADARFIRST IN ACTION

Find out why RadarFirst customer loyalty is industry-leading



Radar® Privacy

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