WHITEPAPER

Radar Privacy

The 3 Challenges to Efficiency in Privacy Incident Response

Patented breach guidance and notification software to simplify compliance with GDPR

The risks associated with data privacy continue to expand in unprecedented and ever-increasing ways. As the number and complexity of breach notification laws accrue, avoiding fines, penalties, and reputational damage due to non-compliance is more crucial and difficult than ever.

Organizations that prioritize these obligations know that security and privacy incidents are both common and inevitable. The true test of incident response management occurs in the actions taken immediately after incident detection, where successful compliance hinges on the speed, consistency, and defensibility of an organization's assessment and notification decisions. From investigation, risk assessment, notification decision-making, and analysis, one of the most important aspects of privacy management is privacy incident response.

Benchmarking Privacy Incidents 2023[1] reveals that 44% of all incidents in 2022 involved paper. Similarly, the vast majority of incidents — 95.2% in 2022 —were unintentional in nature, with only 1.5% caused by malicious actors.

To mitigate risk to their brand, customers, and employees, organizations must learn to centralize incident response within their data privacy initiatives. As global privacy laws tighten, definitions of regulated data broaden, and customer awareness of their data privacy rights increases, a foundation of consistent, defensible privacy incident response allows organizations the confidence to assess risks and make notification decisions without divesting from other privacy, security, or compliance initiatives. Working against competing organizational priorities and inefficient processes, privacy professionals must make the case to rise above arduous, manual processes and usher in the age of incident response automation.

The Privacy Landscape

Privacy has significant business value in today's data-driven economy. As new international regulations become law, analysts predict many organizations will increase spending on privacy.[2] And justifiably so. In addition to meeting compliance requirements and managing risk, a sound privacy program can improve brand value, grow business, maintain public and investor trust, and provide a competitive edge.

When considering ways to operationalize privacy programs, success largely depends on the efficacy of an organization's incident response process. Effective incident response requires a solid understanding of the complex nature of privacy incidents, familiarity with the ever-changing regulatory environment and public perception of privacy, as well as the critical role incident response management plays to reduce risk.

1 https://www.radarfirst.com/resources/2023-privacy-incident-benchmarking-report/
2 https://www.itprotoday.com/data-privacy/data-privacy-still-spending-priority-execs

Industry Threats

The 2022 Verizon Data Breach Investigations Report[3] cited 23,896 security incidents, including 5,212 confirmed data breaches. The findings demonstrate the high prevalence of these incidents (~22%) across all industries and sizes of organizations. Nobody is immune from risk.

Contrary to most headlines that center on electronic, malicious incidents and drive public perception of the privacy space, there are other important areas which organizations need to focus on.

Every incident, whether paper or electronic, malicious or otherwise, must be risk assessed against a mosaic of ever-changing, increasingly stringent regulations to determine if they require notification in the case of a data breach. Breach notification laws are as wide ranging as they are changing, and include various state laws, federal and industry regulations such as GLBA and HIPAA, and international laws such as the EU GDPR and PIPEDA.

Naturally, with increasingly more laws and regulations to anticipate, track, and interpret in order to align internal governance to external regulations, the amount of time privacy officers spend assessing incident risk has increased as well. This creates urgency to arrive at a decision to avoid missing mandated notification timelines. However, an improper risk assessment can result in over- or under-notification or inaccurate notification guidance, putting organizations at risk for fines, loss of consumer confidence, brand or reputational harm to both a company and its employees—in other words, the opposite effects of a successful privacy program.

An effective incident response management program—and consequently a successful privacy program—can be a challenge to put in place. Difficulties in incident detection and escalation, the complexities of breach notification regulations, budget constraints, and process inefficiencies are the everyday realities of privacy pros across all industries.

As the need for quick and defensible risk assessment is not a one-time demand, leveraging automation allows organizations to shorten response time and increase incident response efficiency.

Why Operationalize Privacy Incident Response?

Statistics on privacy risks indicate that cyber-threats and human error show no sign of slowing down in the near future. While these incidents are likely unavoidable for even the most educated and prepared organizations, the challenges of incident response surpass other privacy challenges due to the sheer number and complexity of regulations that entail unique jurisdictional requirements for breach determination and notification in the case of a breach. Coupled with internal policies and third-party obligations, an automated incident response solution provides the consistency and efficiency privacy leaders need to comply with regulatory and contractual obligations.

Let's explore the challenges associated with privacy incident response to better understand how automation helps build a strong foundation to support compliance, security, and legal operations.

CHALLENGE 1

Detection & Escalation

Data privacy incidents come in many forms, each of which involves unique challenges in the detection period. As a result, it's not uncommon for organizations to experience a significant delay between the time of occurrence and discovery, and again from discovery to containment and eventual notification.

3 https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

And who can blame them? After all, organizations that have failed to properly manage incidents in the past become a cautionary tale among their peers and sometimes stay in the public consciousness years after the event. Managing incidents thoroughly and quickly can make or break a privacy team and leave lasting impacts throughout an organization.

When it comes to managing an incident, efficiency and timeliness are key components for compliance. The longer an incident remains unresolved, the more an organization is vulnerable to risk and lapses in compliance.

Many organizations have adopted streamlined methods to identify and report incidents to privacy teams, allowing for a seamless and coordinated solution for incident response management. Since 2020, more than three quarters of respondents to a survey from The Wall Street Journal stated that their compliance programs, "now rely more on data and advanced tools to help them streamline workflows and more quickly flag new risks."[4]

By prioritizing efficiency in incident response processes, teams can reach a notification decision more quickly, leaving more time to provide notice and respond to potential crises.

Radar Privacy metadata revealed in the Benchmarking Privacy Incidents 2023 report, organizations using automation to operationalize incident response take an average of 22.9 days per incident compared to the 2022 IBM Cost of a Data Breach Report[5], which measured organizational process from discovery to notification at 277 days.

CHALLENGE 2

Complex Data Breach Notification Requirements

When an incident involves the disclosure of personal data, the incident includes a dimension of privacy.

Organizations that hold personal data in industries such as finance, insurance, and healthcare must comply with data breach notification laws of each U.S. state, as well as all applicable federal laws such as the HIPAA Breach Notification Rule and the Gramm–Leach–Bliley Act (GLBA) and international regulations such as the EU General Data Protection Regulation (GDPR) and newly established UK-GDPR.

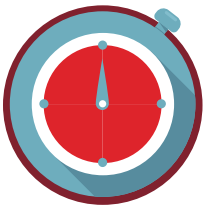
At the domestic level, recent adoption of the California Consumer Protection Act (CCPA) and its recent amendment, the California Privacy Rights Act (CPRA) have given new value to individual rights, which will likely expand to other state jurisdictions as new laws pass in 2023 and beyond.

In light of competing jurisdictional requirements, data privacy laws — especially those with a breach notification component — have grown more stringent, specific, and numerous than ever before.

Several states have joined the group of almost 30 that have passed specific requirements to notify attorney generals in the event of a breach and several more created specific timelines for data breach notifications, requiring organizations to refresh their understanding of notification requirements appropriately for each state regulation.

The constant shifting of regulations makes compliance not a one-and-done activity, but instead requires constant vigilance to keep abreast of changes. And it is this fluid regulatory landscape that challenges even the most diligent organizations and their compliance teams to ensure that internal policies abide by external regulations.

4 https://www.wsj.com/articles/coronavirus-elevates-compliance-risks-for-most-companies-11602149400
5 https://www.ibm.com/reports/data-breach



CHALLENGE 3

The Cost of Inefficiency

The impact of inefficient privacy incident management reaches beyond the breadth of the privacy team's day-to-day activities and extends to the organization as a whole. Without operationalized privacy incident response processes, an organization remains open to unnecessary risk derived from subjective decision-making, inconsistent risk assessment, and the inherent danger of over- and under-reporting.

This risk is compounded by the potential for noncompliance and regulatory fines due to increased time spent from incident discovery to notification decision. And not to be overlooked, third-party contractual obligations often include even shorter notification timelines.

Tactics such as building in-house incident response systems through the modification of existing systems or technology tools requires significant investments of both time and money, in addition to the relentless burden of keeping current with changing privacy laws.

Often such solutions lack the automation and decision-support that both compliance and privacy professionals rely on to determine if an incident rises to the threshold of a notifiable breach. Moreso, these in-house solutions fail to create the incident documentation necessary to support the organization's burden of proof under federal, state, and international regulations, leaving additional work to ensure the breach and notification decisions made were defensible by law.

Amid the COVID-19 pandemic, organizations that invested in incident response were prepared to adapt to new regulations and reaped the benefits of their foresight. Lessons learned from updating processes for GDPR helped equip privacy teams to adapt to CCPA and have proven that sound incident response processes are key for agility and timeliness in the privacy sector.

What traditional approaches to incident response, such as information security, ticketing, and in-house systems don't address is the time-critical requirement to evaluate an incident in the context of applicable laws, determine whether it is a breach, and what notification might be required. Depending on your industry, failure to assess, notify properly, and notify on time can lead to millions of dollars in regulatory penalties plus potential litigation.

For example, in 2022, the average cost of such a breach was $4.35 million, according to a new report from IBM Security.[6]

THE SOLUTION

Consistent & Defensible Incident Response Automation

An operationalized approach to privacy incident response — one that uses automation to map regulations to an incident risk assessment and provide automated notification decision support in the case of a breach — is a critical component to maintaining compliance with ever-changing data breach laws. As a result, this consistent and defensible process further strengthens the foundation of compliance at an organization and frees up time for privacy and incident response teams to focus on other core responsibilities.

The selection of a tool for privacy incident management is made easier when organizational priorities are clear:

- Maintain a strong culture of compliance
- Reduce risk across the organization
- Bolster operational efficiency
- Control costs

6 https://www.ibm.com/downloads/cas/3R8N1DZJ

Conclusion

Organizations that demonstrably value privacy through consistent incident response management will have significant business advantage as the economy becomes even more data-driven. Consumer demand for increased privacy regulation is gaining attention at the state level and regulators are requiring that companies prioritize to meet such requests.

At the risk of reputational harm, diminished customer confidence, regulatory fines, and loss of future business opportunities, organizations are tasked with navigating an increasingly privacy-minded world.

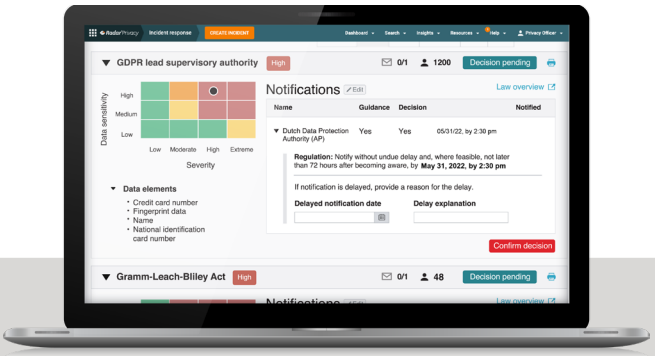
As regulations change almost overnight, the challenges of incident response management continue to increase. Organizations need an efficient, effective, and defensible method for detecting, reporting, escalating, risk assessing, and providing notification on the large volumes of inevitable incidents they experience.

This requires a tool that automates incident response processes in a way that is:

- Consistent for all incident types
- Scalable to easily meet demand
- Repeatable and defensible to meet burden of proof requirements

Multiple software tools exist to help organizations manage their incident response processes. Some include homegrown solutions or generic playbooks and workflows offered by GRC or compliance platforms. While these may have some value, too often they don't provide the automation or clear guidance that is needed for consistent and defensible breach decisioning. An alternative is a purpose-built solution that offers consistent, automated risk assessment and breach notification guidance in compliance with the latest regulations.

When selecting a tool for incident response management, privacy pros should keep their objectives in mind—maintain a strong culture of privacy, reduce privacy risk across the organization, meet growing privacy needs efficiently, demonstrate compliance, and control costs. Then, and only then, will the right choice for a solution become clear.



See how investing in incident response can drive successful privacy programs

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo

RadarFirst

Learn more at radarfirst.com

RadarFirst's award-winning incident management solutions are trusted by organizations in heavily regulated industries to reduce risk and simplify compliance with global breach laws.