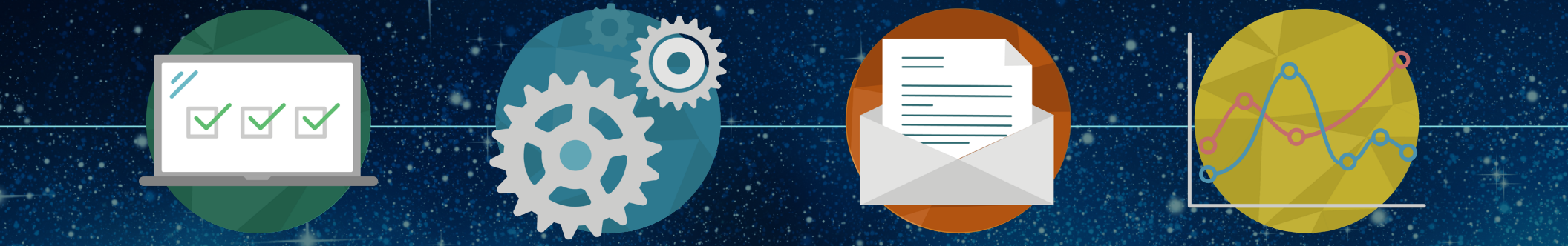


WHITEPAPER

The Definitive Guide to Privacy Incident Response

Radar® Privacy

The Definitive Guide to Privacy Incident Response

Taking Uncertainty out of Privacy Incident Response

Privacy incident response has evolved into a global game of leapfrog: as fast as privacy teams add staffing and improve their processes, new challenges rise before them.

From the US and the EU to Brazil and Malaysia, nations and states are enacting both general and industry-specific privacy regulations. Mandated response times for data breaches are becoming shorter and shorter, despite evolving and disjointed definitions of sensitive information, accountability, ownership of information, and even what constitutes a breach.

We face a growing number of incidents and threats, given the proliferation of data in our business operations, yet privacy teams struggle to get internal commitment and resources, often bundled with or borrowing from non-privacy budget areas such as security.

Table of Contents

To stay compliant in this chaotic environment, you need an incident response process that takes inefficiency and guesswork out of the equation.

A mature incident response process will be:

- **Defensible:** You need to be able to show consistent, objective multi-factor risk assessments and well-documented criteria for your decisions whether to notify or not.
- **Global:** Your risk assessment and response need to take into account all the laws that may apply in each separate incident.
- **Fast and accurate:** Your team needs to arrive at the right notification decision in time to meet compliance deadlines for every applicable regulation and jurisdiction.

To make the best use of resources and to avoid missteps, you need a unified incident response framework, where information flows continuously from incident discovery through post-incident tracking, where automation and analytics are leveraged to help ensure speed and consistency, and where IR is integrated with other processes and tools across an organization.

Some organizations are just finding their way with formalized incident response processes, but even mature privacy programs have areas for improvement. No matter where your organization is on the continuum, this guide is a tool to help you assess each stage of your IR process and identify areas and strategies for improvement.

In the following pages, we'll overview each phase of the incident response process, then give you a checklist to assess whether your organization is executing that phase consistently, effectively, and efficiently, along with possible steps to address performance gaps.

A Unified Framework for Incident Response

A unified incident response process has well-defined phases, each with clear objectives. Consistent, repeatable processes and the right tools to support each phase will help ensure consistency, accelerate decision-making time, eliminate the risk of over- and under-reporting, and help your organization stay current and compliant with the changing regulatory landscape.

Incident Intake and Escalation

An incident is detected by infosec or reported by an internal or external source. The clock is ticking for the IR team to investigate the incident, involve appropriate stakeholders, and capture enough information to drive an accurate risk assessment.

Risk Assess and Decide

Using information gathered during the intake phase, the IR team must accurately determine whether notification to regulators and/or individuals is required based on all applicable regulations in different nations and states.

Breach Notification

If notification is required, the IR team must notify regulators and individuals of the breach in time to meet all regulatory deadlines. Notification must contain the information required in each jurisdiction, and delivery of notifications must be tracked and documented.

Reporting and Trend Analysis

Ongoing analysis is critical to maintain security and to demonstrate your commitment to regulators. Incident sources and severity, consistency of the risk assessment process, and other indicators should be tracked over time and used to pinpoint problems and improve privacy and security processes.

Pre-incident Preparation

Effective incident response depends as much on what you do before an incident as what happens after.

You need an incident response team that's trained and ready to swing into action. You need clear, simple policies, processes, and reporting mechanisms, so that everyone in your organization, from the privacy team to line staff knows how to identify an incident and what to do next. And you need a culture of privacy protection and awareness, so that staff is on the lookout for problems.

Who is involved

Everyone, from the executive suite to the privacy and infosec teams, on to line staff and, ideally, business partners.

Essentials for Success

- ☐ The entire organization is educated about data security and incident response and committed to a culture of privacy.
- ☐ Incident response processes are rehearsed regularly by the IR team with tabletop exercises.
- ☐ Processes and policies are regularly updated to reflect changing regulations, business relationships, and risk appetites within the organization.
- ☐ There is a current benchmark risk assessment in place to help guide and speed post-incident risk assessment.
- ☐ Training in security and incident response is ongoing, including both new hires and existing staff.

Actions for improvement

Here are some actions successful privacy programs are taking for improvement:

- Solicit executive support and involvement to promote a culture of privacy awareness and responsibility.
- Invest in tools that automate regular multi-factor risk assessment and streamline incident tracking. This will help identify and address new and emerging risks and provide data to justify investments to executive leadership. Having a current, baseline risk assessment is also a foundational tool for proving compliance to regulators.

Radar® Privacy ensures access to up-to-date global data breach notification regulations, industry-specific regulations, and proposed or pending regulatory watchlists, going further than other solutions by harnessing automation to operationalize the process, for compliance with new laws and any changes to existing laws.

Incident Intake & Escalation

Effective incident response depends on what you do before an incident, not just what happens after.

Newer regulations have set daunting notification requirements. Under laws such as GDPR, organizations have as little as 72 hours to notify regulators of a possible breach, so incident response processes need to escalate and investigate incidents faster than ever before. This requires a reporting and escalation process that is simple to use and streamlined, but also gathers sufficient, accurate information to support the notification decision.

Who is involved

Core incident response team (privacy, infosec, compliance) reporting staff member or department, forensics.

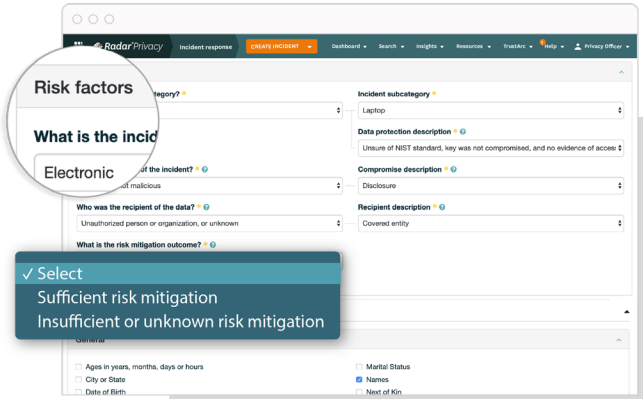
Essentials for Success

- ☐ All staff has access to internal reporting tools and knows how to report and escalate an incident.
- ☐ All necessary incident response team members are promptly engaged and informed.
- ☐ The incident information captured is sufficient to complete an accurate risk assessment.
- ☐ The information-gathering process and tools speed investigation rather than getting in the way.
- ☐ For regulatory purposes, the process establishes clearly when organization is informed/becomes aware of incident/breach.
- ☐ APIs and integrations with the security team's systems (such as SIEM and GRC systems) streamline coordination between security and privacy teams and supply information critical to performing a risk assessment.
- ☐ The information captured becomes part of the permanent incident record in a format that makes it easy to provide regulatory documentation.

Actions for Improvement

Here are some actions successful privacy programs are taking for improvement:

- Institute regular table-top exercises to keep the incident response team in practice. Use tabletop exercises to anticipate new threats or different types of incidents, such as a ransomware attack.
- Deploy a breach response tool with customizable forms to guide information-gathering process and capture information for decision-making and future regulatory, analysis, or legal needs.
- Ensure that processes and tools take account of evolving regulatory requirements such as establishing awareness.



Web forms streamline incident intake and bring consistency to the incident details captured. Radar® Privacy's modern APIs allow for additional automation and system integration, bridging the gap between security and GRC systems for operational efficiency and risk management.

Risk Assess & Decide

The ability to demonstrate a consistent approach is a critical factor in making defensible notification decisions to regulators.

But consistency is challenging. Besides the human factor—differing perceptions of risk within the privacy team—you must deal with the patchwork of global data breach laws, each with different definitions of data breach, personal data, exceptions, notification thresholds, and notification timelines. When an incident involves the sensitive data of individuals from multiple regions of the globe, your risk assessment process must be consistent, efficient, and effective according to all applicable law to ensure compliance and avoid over- or under-reporting.

Who is involved

The core incident response team (IRT), counsel, marketing/PR, finance.

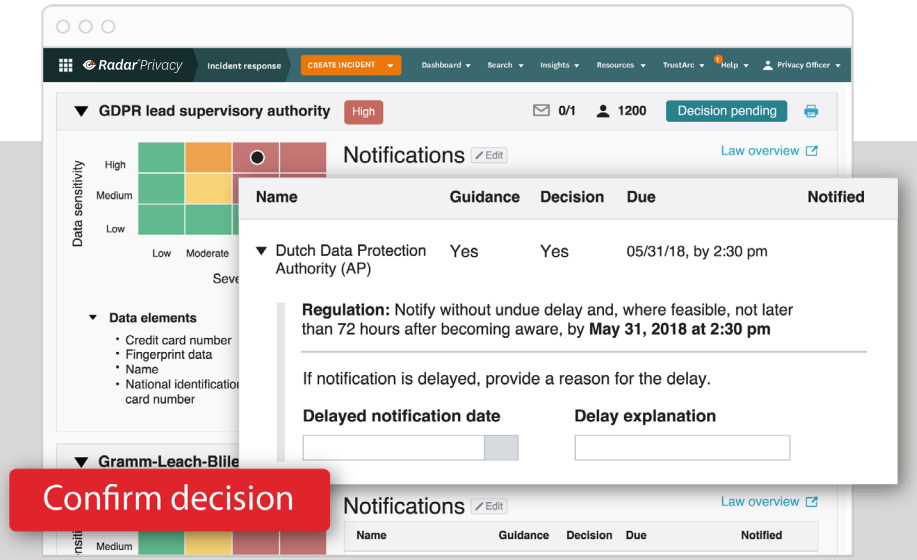
Essentials for Success

- ☐ Your risk assessment is based on complete, up-to-date application of all applicable regulations and jurisdictions, as well as contractual obligations.
- ☐ Decisions are based on consistent criteria for assessing risk of harm to individuals and the organization.
- ☐ Over time, process leads to a reduction in over-reporting or under-reporting.
- ☐ After a determination whether to notify regulators and/or individuals, the decision criteria are documented for future regulatory, analysis, or legal needs.
- ☐ The reason for your decision is fully documented, whether you decide to notify or not.

Actions for Improvement

Here are some actions successful privacy programs are taking for improvement:

- Deploy tools to provide decision-makers with an up-to-date knowledge base of global privacy laws and regulations and to automatically document decision criteria.
- Conduct on-going analysis of decision results and tune decision-making criteria to avoid over- or under-reporting and reinforce consistency across assessments.



Radar® Privacy applies current state, federal, global, and contractual notification obligations to profile each incident, providing consistent incident risk scoring and decision-support guidance.

Based on the guidance provided by Radar® Privacy and your privacy policy, you make the ultimate decision to notify or not. Either way, the entire process is documented.

Breach Notification

If you determine that notification is required, your privacy and legal teams have to be ready to quickly generate notification letters to individuals, regulatory agencies, and data protection authorities, as well as track responses and document their efforts.

They also have to maintain counsel-approved notification letter templates and ensure that each notice meets regulatory and contractual requirements, as well as the strategic needs of your organization.

Who is involved

The core incident response team (IRT), counsel, marketing/PR, finance.

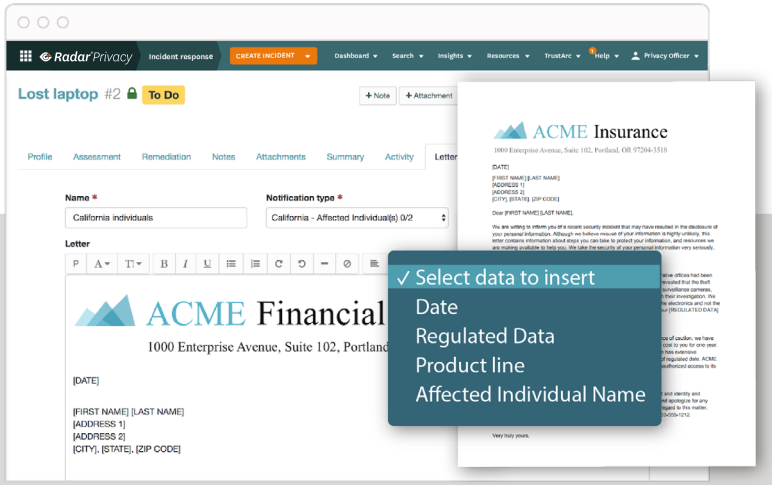
Essentials for Success

- ☐ Your IR automation tools provide alerts for notification deadlines, formats, and content requirements.
- ☐ Your team can create and manage notification letters using pre-approved templates and leveraging automation to fill in any required incident data.
- ☐ The notification process creates a central repository of all notifications to improve compliance.
- ☐ Response progress is tracked accurately and automatically after notifications have been sent.
- ☐ All notification letters become part of the incident documentation.

Actions for Improvement

Here are some actions successful privacy programs are taking for improvement:

- Review notification templates regularly to ensure that they meet evolving regulatory requirements.
- When establishing notification templates, have counsel and PR review notification letters to ensure they meet your organization's strategic needs.
- Deploy tools to automate the notification process, with deadline alerts, templates, notification tracking, and reporting.
- After an incident, regularly review reports on notification delivery and follow up as needed to ensure compliance.



Radar® Privacy helps you meet breach notification deadlines with built-in and fully customizable notification letter templates. And a central repository for storing all incident-related documentation helps you quickly and easily prove compliance to regulators and auditors.

Reporting & Trend Analysis

The time after an incident is also the time before the next incident—time you can use to evaluate and improve your incident response process and to pinpoint and fix gaps.

Identify areas the process could be accelerated. Analyze past incidents to compare causes and factors and spot problem areas. Look at incident response metrics to see whether you're consistently meeting regulatory deadlines and to see whether you're tending to over- or under-report. And don't forget to measure and celebrate successes and improvement. Take the opportunity to highlight your progress and convey your ongoing needs to your executive leadership and Board.

Who is involved

Core incident response team (IRT), privacy team, infosec, HR/training, executive team (informed).

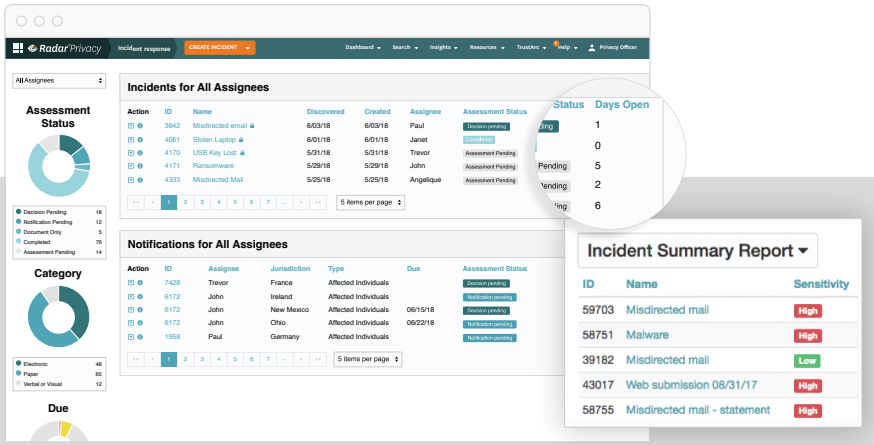
Essentials for Success

- ☐ Your privacy team has real-time reporting and data visualization to help spot emerging trends and trouble spots.
- ☐ There is regular reporting of key metrics and trends to executive staff and other stakeholders.
- ☐ Learnings are consistently applied to address security gaps and to improve privacy programs and incident response processes.

Actions for Improvement

Here are some actions successful privacy programs are taking for improvement:

- Choose tools that provide a real-time dashboard of incidents and response, with trend analysis and customizable reporting.
- Compare your program against industry benchmarks.
- Conduct and document periodic, enterprise-wide risk assessments to spot new areas of risk.
- Convene regular meetings of privacy teams, infosec, and other stakeholders to review performance and trends, create action plans to address problems, and review progress.

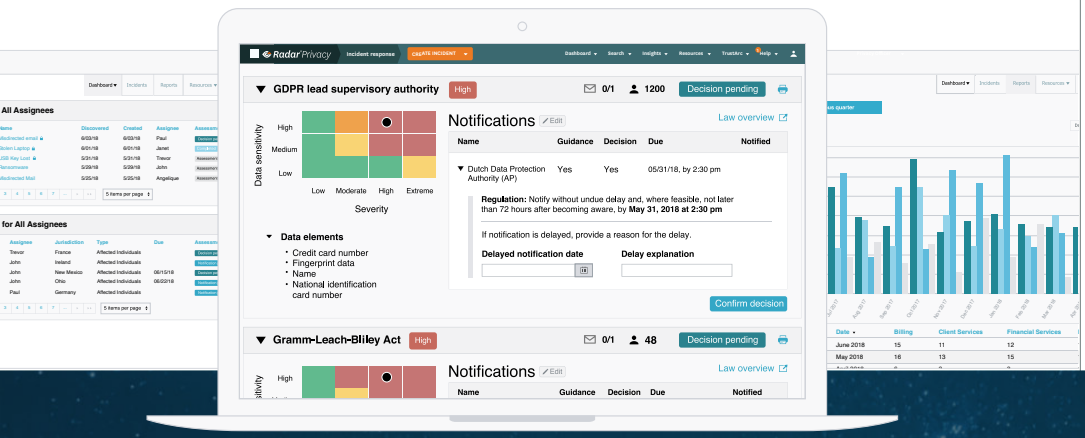


Build reports and identify trends directly in the Radar® Privacy platform. With data visualization, dashboards, and benchmarking built-in, you can easily pinpoint areas of improvement and pull reports for leadership and the board.

Conclusion

How you do incident response is vitally important, not only for compliance but for protecting your customers and your organization. Whether your organization, your privacy team, and your resources are large or small, you need to strive for an IR process that is fast, efficient, and leads to decisions that are defensible to regulators and effective at protecting affected individuals.

You can't prevent every incident or breach, but with commitment and the right tools, you can use each one as an opportunity to improve.



Additional Resources

Breach Law Library

Access this free library of hundreds of global privacy laws, rules, and regulations to stay current on existing and proposed legislation.

Access the Regulatory Law Overviews »

Regulatory Guides

Get in-depth information on key regulations such as CCPA, GDPR, PIPEDA, and Australia's Notification Data Breaches scheme. Includes comparison guides.

Access the Guides »

Incident Risk Assessment Simulator

Take a tour through Radar® Privacy's patented multi-factor risk assessment engine. This simulator automatically assesses the risk of common data privacy incidents to demonstrate the efficiency, consistency, and risk mitigation benefits of its purpose-built technology.

Assess an Incident »