# HOW TO FIX AN

# INCONSISTENT, MANUAL and PAINFUL

## Incident Response Process

RadarFirst

# How to Fix an Inconsistent, Manual, and Painful IR Process

## A Strategic Approach to Incident Response

In today's **threat landscape**, privacy-related incidents are inevitable, and in today's **regulatory climate**, you are required to have an incident response plan and process. But incident response is about more than compliance.

The quality of your processes and tools also determines how your organization will fare in the event of a future audit or legal action. If your practices are designed to let you track and analyze incident and response trends over time, you can use them as metrics to achieve continuous improvement in both privacy and security.

In this paper, we look at best practices from several leading financial, healthcare, and governmental organizations to see how they use incident response as a springboard to improved incident response management practices and results.

## The Challenges of Incident Response

Ten years ago, most organizations were coming to grips with the necessity of having an incident response plan. Today, they are coming to grips with the fact that privacy and security incidents are an almost-daily occurrence. The explosive growth of cybercrime has increased both the number and the variety of security threats to personal information. The attack surface has expanded exponentially with the growth of mobile access, cloud computing, and the billions of mostly unsecured, connected devices that make up the "Internet of Things."

Despite the increasing technical sophistication of both threats and defenses, people remain the weakest link in our defenses, whether falling prey to social engineering campaigns, unwittingly transmitting malware into networks, willfully committing insider theft, or simply failing to secure protected information. So in addition to improving

RadarFirst

## Outline



## About the Individuals Quoted in This Guide

The following best practices come from a series of interviews with RadarFirst customers and partners, from leaders in privacy at Fortune 1000 financial institutions, government agencies, health systems, and global law firms.

Keeping these conversations confidential allowed interviewees to respond candidly regarding their organization's approach to privacy.

Privacy is a top concern at RadarFirst –it's why we're in this business, and what our platform is built on.

information security, organizations must continuously train and monitor employees–and they should demand the same from their service providers and business partners.

In parallel with growing privacy threats, regulations have changed and become more stringent. Compliance now means navigating a maze of constantly changing state, federal, and international regulations.[1] A partner at a global law firm told us she focuses on privacy and data protection in her practice, and that even she finds it challenging to keep up. She points out that not only do most states have their own privacy laws, but different statutes set different thresholds and timelines for breach notification—with different requirements for specific content and format in notification letters.

Additionally, we're seeing a trend of regulatory agencies like the Department of Health and Human Services Office for Civil Rights (OCR) levying fines on organizations who fail to meet the timelines associated with their notification obligations. For example, early in 2017 Illinois-based Presence Health made a $475,000 settlement with OCR for waiting 41 days past the notification deadline to inform officials of a HIPAA violation that led to a breach of unsecured protected health information of more than 800 individuals. In addition, businesses across the globe will face penalties of up to 4% of global annual revenue for non-compliance with the General Data Protection Regulation (GDPR), which takes effect in May of 2018.

With the expanding and volatile risk picture, organizations are struggling with several questions:

- How to ensure consistency when assessing incidents for breach determination and reporting (Arguably the single most important challenge for most organizations)
- How to make incident response processes efficient, scalable, and cost-effective
- How to keep up with and meet changing regulatory deadlines and requirements in a timely way and while containing legal expenses
- How to promote communication among siloed teams (security, compliance, privacy, legal, etc.) so that incidents don't slip through the cracks

As they face these challenges, more organizations are also beginning to ask the strategic question: how can we leverage our incident response processes to better manage our risks, assure compliance, control breach costs, and improve our privacy and security posture.

So let's look at how some successful privacy and compliance teams are answering those questions.

**To meet your burden of proof, it's important to demonstrate consistency and to document your risk assessment and remediation actions.**

## The Basics: Consistency and Compliance

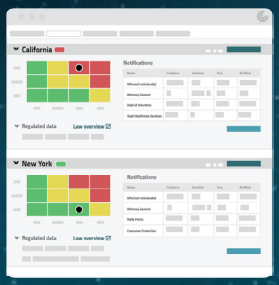
When assessing an incident, it's important to consistently consider multiple risk factors to make the best decisions that protect your organization and those affected by the incident. Protecting the organization begins with regulatory compliance because, while the majority of incidents can be adequately remediated and are determined not to be breaches after a multi-factor risk assessment, without proof of compliance your organization can still face regulatory violations, corrective action plans, and substantial penalties. To meet your burden of proof, it's important to demonstrate consistency and to document your risk assessment and remediation actions.

The first step towards a consistent incident response process is to have a process, preferably an easy and efficient process for all employees to report new incidents with all the relevant information as necessary.

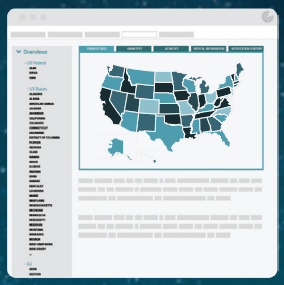
## How RadarFirst Automates Incident Response

Top-level overview of all open incidents reported through your organization, to quickly determine which incidents might need attention

Consistent process document all the key information, pertinent to a multi-factor risk assessment.



Assessment results provide consistent, jurisdictional guidance as to whether an incident requires notification to various agencies and impacted individuals, with a heat map displaying data sensitivity against incident severity.



The results displayed after an incident is assessed always include the latest breach notification laws across supported jurisdictions.

Easily display trending data for incidents across many category variables, with the ability to customize the display by incident and category variables, chart type, and date range. You can also export the data for further analysis.

Otherwise, incidents can be missed, response decisions may be delayed or made based on incomplete information, and if auditors come knocking, you can't explain what you did or why. The Chief Privacy Officer at a large financial group, recalled the world before her team established a repeatable incident response process: "Everything was ad hoc, case by case. Someone would call me asking "Is this a problem." It makes my hands sweaty just to think about it."

> "We look at RadarFirst as a source of truth. In fact, when we get an incident, we say 'Let's run a RadarFirst on it.'"

The second step is to ensure that you're assessing incidents in a consistent, compliant way that takes into account all the current applicable regulations and contractual obligations. Many leading organizations have turned to the RadarFirst purpose-built incident response platform to help them ensure consistency, to provide a decision support framework for compliance, and to operationalize a strong culture of compliance and privacy.

RadarFirst is a software platform that combines an up-to-date knowledge base of state, federal, and international privacy regulations with built-in risk assessment algorithms to help determine whether a privacy or security incident rises to the level of a notifiable breach. Privacy and compliance teams find that RadarFirst helps them stay current with constantly changing breach laws, and it helps them consistently assess and document all incidents while facilitating oversight by counsel, when necessary.

Using automation in the multi-factor risk assessment process helps assure consistent and defensible decisions. The Information Privacy Manager at a major non-profit health system and insurance provider recommends using RadarFirst for every incident and following its decision support guidance unless you have a very good reason not to do so. She says, "We look at RadarFirst as a source of truth. In fact, when we get an incident, we say 'Let's run a RadarFirst on it.'"

Interestingly, just the fact that you are using a purpose-built tool can help prove compliance. A former Privacy Incident Coordinator for a state agency says that, when faced with a federal audit several years ago, the agency was able to pass the audit by demonstrating that they were implementing RadarFirst to close any gaps and ensure compliance.

When using RadarFirst to help automate incident risk assessment, there will be some judgment calls in how you characterize an incident when using RadarFirst to capture the incident's risk factors. One healthcare privacy specialist gives an example:

***"Let's say an employee inadvertently receives protected information from another employee in the course of their work. How do we describe that when answering incident risk factor questions in RadarFirst?"***

For common types of incidents, her privacy staff gets together to determine predefined answers to questions in the tool so similar incidents are profiled according to established criteria ensuring consistency in risk assessment. For more uncommon, outlier incidents, they sometimes consult counsel or check with state or federal regulators on how to proceed. Once a decision is made, they document it, create an incident risk factor template, and educate staff so that they can use the tool in a consistent manner the next time a similar incident occurs.

Organizations that adopt RadarFirst also report that it helps them scale incident response without overloading staff. The Chief Privacy Officer for a Fortune 1000 finance and insurance company says that before adopting RadarFirst, her group didn't have the capacity to manage day-to-day incidents, and other privacy teams say they had reached their limits with the ad hoc, often spreadsheet-based processes they were using before they deployed RadarFirst.

In addition to having the right tool, experienced privacy professionals recommend that you make it a practice to assess every incident, large or small. You'll need to teach IT and business staff to report all possible incidents rather than using their own judgement. In fact, most privacy professionals we talk to say they encourage their employees to over-document rather than under-document, so they can ensure that each incident receives a proper multi-factor risk assessment. The Director of Privacy and Security at a major university medical center recommends making incident reporting available through web-based forms so that it's easy for people to report incidents right away from wherever they are working.

## Document to Prove Consistency

Many industries, including finance and healthcare, have regulatory reporting requirements after a data breach, and some regulatory agencies expect monthly and quarterly reports and conduct periodic audits. In an audit, you need to be able to prove that you have a culture of privacy and compliance by demonstrating consistency throughout your incident management lifecycle–and that requires documentation. The legal landscape is also changing because of precedent-setting rulings that are allowing breach victims and business partners to claim damages,[2] so the documentation you use to show compliance can also be invaluable to your defense if a breach leads to legal action. It's nearly impossible to assemble all that information after the fact, so documenting should be built-in as part of your breach response process.

**Experienced privacy professionals recommend that you make it a practice to assess every incident, large or small.**

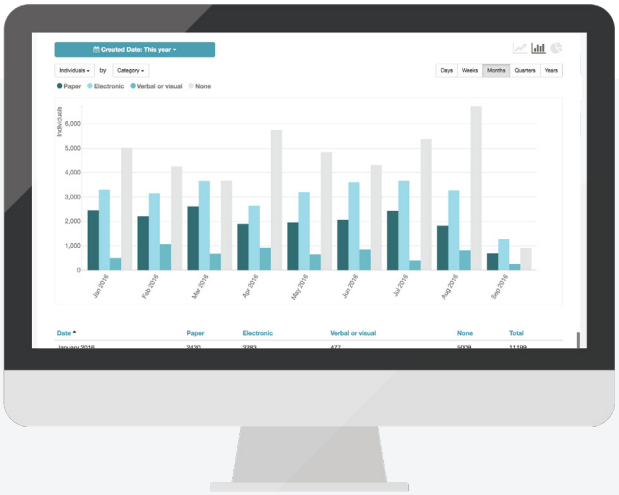
One government privacy expert points out that auditors want proof of consistency in multi-factor risk assessments

and notification decisions, so you should have complete documentation on each incident. Her team uses RadarFirst to document every aspect of their decisions as they conduct incident assessments. They even document incidents that clearly fall outside of regulatory requirements, just to have all the information in one place. She says that if you decide to override or modify a recommendation by your incident response platform, fully document the reasons you made that exception. And if you choose to notify voluntarily on an incident where notification isn't mandated, she says to document that too, because that helps show auditors that you err on the side of compliance.

The privacy and security team at a major healthcare network have made sure that their organization's commitment to privacy and security best practices includes third-party vendors in both incident response plan and in documentation. They are bringing contract management into a centralized process, and plan to document security and privacy terms with vendors in their RadarFirst system so that they can take contractual notification obligations into account in their incident assessments. They are also instituting a process to ensure and document that any protected information held by a vendor is destroyed when that relationship is terminated.

If you face an audit or legal discovery proceedings, there will be deadlines for providing incident response documentation. To help meet those deadlines, the healthcare privacy team mentioned above has developed documentation listing the information that will be required in an OCR audit (healthcare privacy) and where it can be found in their RadarFirst system. They also use RadarFirst to get a jump on OCR reporting requirements for the year. The team used to send OCR information annually on reportable incidents involving less than 500 records, but they found they were getting backlogged. Now they report immediately. One senior privacy specialist says he generates reports as soon as he finishes his risk assessment and decision making in the RadarFirst system: "I have my RadarFirst document, I have my OCR web page open, I have all the information there, and I just complete it all at the same time."

**Your incident response process can be a springboard for continuous improvement if you track key performance indicators and conduct regular reviews of incidents and trends.**



**RadarFirst's reporting feature allows for visualization of your privacy program's efforts, an effective means for a privacy team to communicate with senior management and to ensure focus and funding for privacy.**

## Use Data for Continuous Improvement

Successful privacy and compliance teams recognize that every incident is a learning opportunity, a chance to become more efficient and effective at protecting personal information. As one insurance industry CPO says, "We don't like wasted pain. If we're going to have an incident, we want to see if we can change things so it doesn't happen again." Your incident response process can be a

springboard for continuous improvement if you track key performance indicators and conduct regular reviews of incidents and trends.

First, be sure your process and tools yield performance metrics so you can analyze and see patterns over time, both problem areas and opportunities for improvement. RadarFirst's robust dashboard can make it easy to get the data you need. Each privacy and compliance team needs to decide what metrics are most relevant to their business.

For example, one team we interviewed reviews the top five incidents of each quarter, incident volume by quarter, number of affected individuals by quarter, and the root cause of incidents by department. A government privacy team holds reviews every 6 months, looking at volume of incidents, originating location, risk level, incident type, increased incident activity and risk levels, and for signs of under-reporting such as a sudden, unexplained drop in incidents from a particular source.

Here are some typical key performance indicators that privacy teams track:

- Average times from when an incident is discovered to:
  - *When it is reported to the privacy office*
  - *When a report is created in the incident response system*
  - *When a multi-factor risk analysis is completed*
  - *When the incident case is closed*
- The percent of incidents requiring mandatory notification due to regulatory requirements or contractual requirements
- The percent of incidents requiring notification in multiple jurisdictions
- The frequency of missed notification due dates
- Trends in incident volume by category (e.g., electronic vs. paper), the type and number of records, the incident source (e.g., internal vs. 3rd party), and by root cause

Incident data analysis and benchmarking are also the most effective means for a CPO or CISO to communicate with senior management and to ensure focus and funding for privacy. A senior privacy specialist in healthcare meets quarterly with the CEO of the hospital and medical center where he's based to provide a report on incident response metrics and cases in progress. He also shares metrics with business unit managers so they can measure themselves against the rest of the health system on privacy and security performance. Integration between the incident response platform and enterprise GRC systems can also help increase the visibility of privacy and compliance programs.

Most importantly, proactive privacy teams use incident response information as a catalyst for action. Trends in root cause data can indicate information security holes or security gaps in business processes. Tracking where incidents originate can point out problems with security awareness or skills in different areas of the organization. For example, many teams conduct annual security training for employees, but proactive ones also do on-demand training during the year if they see a department with an unusual number of incidents.

**Proactive privacy teams use incident response information as a catalyst for action.**

Many privacy teams report that more training has a side benefit: more incident reporting. After one healthcare privacy team held training to address specific problems, they saw an increase in the number of incidents reported, but a drop in the number of breaches that required reporting to OCR. One government privacy expert says she always looks for an increase in incident escalation and reporting after training; in fact, she considers it a sign of success.

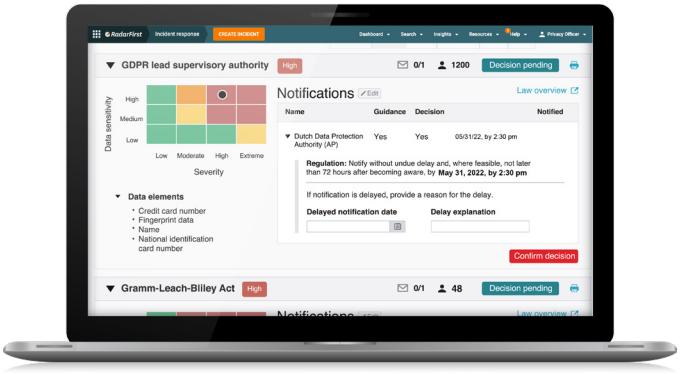
## Focus on the Big Picture

Compliance is important, but incident response is ultimately about mitigating incident and breach risks and being more effective in your defenses.

More than anything, successful privacy teams foster an enterprise-wide culture of privacy and compliance in their organizations, and they use data to persuade the board, C-suite, and business managers to set the tone on privacy programs. One CPO summed up her organization's philosophy this way:

***"Privacy is everybody's job, and it's bigger than a compliance issue: it's a business issue because it's about trust. If your business depends on relationships with people, then your success depends on your ability to do a  good job at privacy."***

Good incident response practices are critical to compliance, but they are also a vital part of this larger picture. Done right, incident response can inform and improve privacy programs as much as it supports compliance.




## Demo RadarFirst Live

A demo of RadarFirst can show you how the pros conduct risk assessment.

**INFO@RADARFIRST.COM | 1.844.737.3778**

**See RadarFirst in Action**

RadarFirst

Learn more at radarfirst.com

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