RadarFirst

GUIDE

Buyer's Guide to Choosing an Incident Response Management Platform

Incident response management platforms (IRMP) are a new, but fast growing technology designed to simplify, automate and ensure regulatory compliance when responding to privacy and security incidents. Effective IRMP solutions must provide efficient risk-based management of incident response lifecycle including regulatory and contractual guidance.

When considering your IRMP options, you should ensure that the platform provides the following core capabilities:

1. **Consistent Incident Assessment & Breach Guidance** - Must perform multi-factor risk assessment that meets federal and states regulatory standards. And provides consistent decision-support guidance about when to provide breach notice. A solution that does not provide defensible guidance fails this most critical requirement.

2. **Purpose-Built Workflows** – Workflow must be specifically built for automating and managing the unique complexities of incident response lifecycle, including:

- **Regulatory Obligations** - Automated incident escalation, multi-factor risk assessment and notifications in compliance with federal and state breach laws.
- **Contractual Obligations** – Workflow for managing contractual obligations with your clients and/or vendors and provide analysis of your level of compliance for proper risk management.

3. **Flexible, Scalable & Configurable** – Out-of-the-box flexibility and user customization to support your organization's culture of compliance and policies.

4. **Intuitive & Easy-to-Use** – It's important to make sure your incident response platform is highly intuitive and can be used by sophisticated and novice users alike with a high level of user confidence and satisfaction.

5. **Cloud-Based** – On premise solutions cannot keep up with frequent regulatory updates and are impractical and too costly for your IT team to manage. A purpose-built IRMP solution requires a secure, agile development and deployment model that is managed and maintained by the vendor.

6. **Secure** - When selecting an incident response platform, confirm that it follows best practices and industry standards for application, network, and infrastructure security

7. **Interoperability With Other Systems** – Ensure that the platform offers web-based application programming interface (API) to enable easy integration and exchange of data with other systems within your environment, including GRC, SIEM, and incident ticketing systems.

8. **Reporting** – Ensure that the system has a flexible reporting framework that enables standard and user defined reports and allows exporting of the data for use within your other business intelligence applications.

9. **Support** – Make sure that the system has proven support metrics, including on-boarding, training and on-going issue resolution. Ask for references.

10. **References** – Last but certainly not least, you must ensure that the vendor can provide highly satisfied references from within your industry and peer group.

About Radar®

In today's world of increasingly complex and changing privacy regulations, cyber attacks, and data breaches, leading organizations trust Radar®, a patented SaaS-based incident response management platform that simplifies and streamlines compliance with federal and state data breach laws. The Radar Breach Guidance Engine™ leads users through an intuitive workflow that profiles and scores data privacy and security incidents and generates incident-specific notification guidelines to help ensure compliance with federal and state laws. Fortune 100 companies and other organizations from heavily regulated industries in finance, healthcare, insurance, and beyond rely on Radar for an efficient and consistent process for incident response. Learn more at radarfirst.com.