RadarFirst

COMPARISON GUIDE

Compare Incident Response Management Solutions

Selecting the best option

Data—big or small—and the vulnerable environment in which it lives has evolved so quickly that organizations can barely keep up. Growing threat vectors and actors can take down a system, exposing personal data to theft and loss. As recent data breaches prove, companies are lagging in their preventative controls. It's no wonder, then, that the 2015 Verizon Data Breach Investigations Report cited 79,790 security incidents from only 70 organizations.[1] That's 1,140 incidents per organization per year.

How an organization manages its response to these data incidents determines the level of risk to its business, brand, and customers. To be successful, companies must develop an incident response process that accounts for the evolving nature of threats, copes with limited resources, and complies with complex breach notification laws.

Options for Incident Response Management

Many types of software tools exist to help organizations manage their incident response process. These range from homegrown solutions to workflows offered by GRC or compliance platforms to an emerging class of software that is purpose-built for managing incident response. This guide explores each of these three options, and provides criteria for making the best decision for your organization's needs.

Option 1: Homegrown Solutions

Ad-Hoc Incident Response Management

This reactive approach happens when a company has no set strategy for managing incidents. Although organizations can rely on external legal and operational expertise and resources to help manage their incidents, the lack of a consistent internal process puts companies and their customers at risk for brand damage, lost business, identity theft, and lawsuits or fines. In addition, the ad-hoc approach does not meet the requirements of incident response management under HIPAA, GLBA or state laws. In the long run, this seemingly low-investment approach can be the costliest.

> "The findings of our research [in the *Cyber Security Incident Response* report] suggest that companies are not always making the right investments in incident response. As a result, they may not be as prepared as they should be to respond to security incidents. One recommendation is for organizations to elevate the importance of incident response and make it a critical component of their overall business strategy."
>
> – Dr. Larry Ponemon,
> Chairman and founder of the Ponemon Institute

Decision Trees (Paper/Excel)

Paper-based decision trees are the first-generation of tools developed by privacy and compliance professionals to cope with the complexity of federal and state breach notification rules. Whether homegrown or consortium-grown, decision trees and associated checklists do not provide consistent and scalable incident assessment or ease of use. They lack the automation to efficiently track federal and state obligations, or to standardize best practices for incident response management. Organizations must use additional means to document and demonstrate compliance internally and to regulators.

Option 2: Multi-purpose Software Suites

One source defines software suites as "related programs that interact nearly seamlessly with each other to make certain tasks easier among different programs."[2] Businesses find them useful for many jobs, such as auditing information systems, creating digital media or performing GRC-related tasks. Often, however, software suites don't have the in-depth functionality to do complex or highly specialized tasks, such as incident vv management. For instance, developers of many GRC and compliance solutions have included incident response management as an add-on, and not a core competency.

Governance, Risk and Compliance Solutions

GRC applications address enterprise-level governance, risk and compliance issues. Despite their wide range of features and functionality, they lack the depth and focus on incident response management found in a purpose-built solution. Most GRC applications are not designed to keep up with evolving regulations, lack a consistent and reproducible method for incident assessment, and do not provide the guidance needed to respond appropriately to incidents. Thus they fail to meet organizations' burden of proof under HIPAA/HITECH, GLBA or state breach notification obligations. These platforms also require significant investment to implement and maintain.

Compliance Management Tools

This class of software applications helps organizations meet compliance requirements, including meaningful use, quality management and HIPAA compliance gap analysis. These tools use their case management features for managing incident response. However, they fail to address the incident assessment and safe-harbor provisions of federal and state breach notification laws. Without the ability to perform assessments, compliance management tools cannot determine if an incident is a reportable breach, and thus help organizations plan for an appropriate response.

Option 3: Best-of-Breed Incident Response Management Software

This class of software is purpose-built for incident response management. As with other categories, each provider has its own focus. Some software offers workflow and functionality primarily for security professionals, while others encompass the privacy and security aspects of incident response management. The latter type of software guides privacy, compliance and security professionals through the maze of state and federal regulations to determine if the incident is a notifiable breach. This software provides notification requirements, documentation, reporting, trend analysis and support for any ensuing regulatory audits or investigations.

This functionality improves workflow for managing incident response in several ways; for instance, all members of the workforce can report incidents by customizable web interfaces. Because it is delivered as software as a service (SaaS), incident response management software can stay current with changing laws, and implementation and maintenance have little to no impact on an organization's IT resources. This option conforms to security best practices to ensure compliance with regulatory requirements and with an organization's security standards.

Why SaaS ?

SaaS applications are usually stored in the cloud, and thus have several advantages over more traditional solutions:

- Faster, easier time to market
- Lower cost of ownership
- Highly scalable
- Little or no downtime
- Can be integrated into existing systems
- Greater security
- Constantly updated and improved
- No maintenance

Which Option is Right For You?

When choosing a solution for incident response management, be sure to identify and prioritize your organization's requirements and then evaluate each solution against the appropriate criteria. Also remember that the risk of improper incident response affects organizations in every industry and of every size. Whether you are a standalone hospital, large financial services company or a local retail chain, you have a legal and ethical responsibility to protect your customers or patients. To help you meet your obligations, we recommend the following criteria when evaluating options:

- Incident response timeline: Tracks significant events of an incident for accurate reporting and notification to regulators and affected individuals.
- Up-to-date federal and state regulations: Ensures proper response—including notification—based on latest laws, reducing chances of fines, lawsuits, and regulatory investigation.
- Wizard-based interface: Guides users step-by-step through incident reporting and assessment processes.
- Trending and analysis reporting: Reduces breach risks by identifying and analyzing where and how incidents are occurring.
- Consistent incident assessment: Ensures all incidents—regardless of size, cause, or other factors—are assessed the same way, every time.
- Web-based incident submission forms and alerts: Enables all members of your workforce to report incidents anytime, anywhere.
- Breach Guidance Engine: Provides workflow for determining if an incident is a reportable breach.
- Patented technology: Demonstrates provider's commitment to ongoing innovation, improvements and enhancements.

Compare Your Options

	Purpose-Built Software	Multi-Purpose Software	Homegrown Solutions
Incident Response Timeline	X	X	X
Up-to-date federal and state regulations	X	X	X
Wizard-based interface	X	X	X
Trending and analysis reporting	X	X	
Consistent incident assessment	X		
Web-based incident submission forms and alerts	X		
Breach Guidance Engine	X		
Patented technology	X		

The Best Option

With its rich functionality and ease of use, purpose-built software for managing incident response is a wise investment for organizations. Little to no maintenance and frequent updates make it easy for security and privacy professionals to integrate this software into their organization's IT infrastructure. In addition, incident response management software offers the guidance, workflow and insight needed for organizations to fully manage incident-related risk.

Selecting the Right Incident Response Management Solution

If you decide purpose-built software for incident response management is the right solution for your organization, it is important to remember that not all solutions in this category are created equal. You want software from a reputable provider that meets the following criteria:

- Engine that provides actionable guidance
- Scalable
- Easy to use
- Always up to date with current regulations
- Cloud-based
- Secure
- Low maintenance

Radar®

Radar meets all of these requirements, bringing simplicity and efficiency to incident response. Radar guides you through the process of characterizing, assessing and responding to incidents so you can ensure your regulatory compliance and reduce breach risks. It captures and creates a profile of incident information so it can be assessed using its patented Breach Guidance Engine. Using insight from the engine, you can determine if an incident is a breach, then, if needed, follow the guidance to respond to the incident and prove your compliance. Radar's Breach Guidance Engine™ ensures all incidents are assessed consistently.

Radar's efficient workflow allows multiple users across the organization to collaborate, and its central repository stores documentation and reports for easy access in case of an audit or investigation. In addition, Radar's reporting features help reduce security risks by pinpointing and analyzing incident trends and root causes.

End Notes

1 Verizon 2015 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2015/

2 http://www.wisegeek.com/what-are-software-suites.htm

Talk to an expert

855-733-9888

info@radarfirst.com

Learn more online

www.radarfirst.com

@radarfirst

Radar

About RadarFirst

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.

© Copyright 2016 RadarFirst. All Rights Reserved. 0919