Buyers guide

Data breach notification tools: A discussion

Are your security and privacy teams prepared to address breach reporting requirements? Do your tools provide cyber resilience? Evaluate your options with these questions.

IBM Security

IBM

Considerations for your security incident reporting

Your organization may need to comply with a complex range of data breach reporting requirements. Driving these regulations are a loss of personal data or personally identifiable information (PII) and a loss of availability of a critical service. Security incidents and some level of data breach can contribute to the volume and severity of cyberattacks against many companies.

To help address these issues, your enterprise should work toward achieving a high level of cyber resilience—the capacity to maintain its core purpose and integrity amid cyberattacks. IT and security professionals measure a company's cyber resilience by the ability to detect, respond and mitigate the impact of cyberattacks.

A 2019 Ponemon Institute study, sponsored by IBM Security, found that 66 percent of organization leaders surveyed consider aligning privacy and security operations teams to be essential or very important to achieving cyber resilience for the following reasons:

- Reduces silo and turf issues
- Improves efficiency in privacy and cyber operations
- Achieves compliance with data protection regulations[1]

Managing and responding to privacy breaches typically involves more than your security team. Privacy, legal and marketing communications employees and senior executives might need to coordinate and respond in a timely manner. Technology can assist in driving this coordination, so that all stakeholders can have a clear understanding of their respective roles and responsibilities and what actions they need to take.

A common trend among data protection regulations is a specific timetable for the initial reporting requirement. The most well-known example is the European Union's General Data Protection Regulation (GDPR), which requires organizations to notify the relevant Supervisory Authority (SA) of a breach within 72 hours.[2] To help meet this short deadline, speed and accuracy should be part of your response process.

To help determine if you have the tools and processes in place to perform data breach preparation, assessment and management, review the following quiz about some of the available features that can apply to your operations. Answers reflect a selection of example solutions and aren't exhaustive of all possible solution types that may be available.

11.7 billion+

leaked or stolen records in publicly disclosed incidents from 2016 through 2018[3]

How does your security incident management tool function? 1

□ **The solution offers options for review and oversight of data breaches, although the processes don't always work together.**
1 point

Minimal connections
Knowing problems existed without having a single system of record to show how and when you addressed each breach can present a time-consuming headache for your security team members having to address state, federal and industry regulations.

□ **The tool provides insights on potential risks of data breaches and a record for auditing without aligning the information between your privacy, legal and security operations.**
2 points

Lack of communication
This setup can allow for discrepancies among members of your operations in response time and approaches to handling data incidents. Crucial information may not be shared between all parties in this area.

□ **The platform provides a single point of management for data breach preparation, assessment and management, which is tightly integrated with security operations for efficiency.**
3 points

Coordination throughout your enterprise
The use of security orchestration together with automation in technical and privacy-related breach tasks can help your response team gain visibility.

What data privacy reporting regulations does the management platform survey? 2

□ **The tool reviews data breach laws for every state in the United States and industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the New York Department of Financial Services (NYDFS).[4]**
1 point

No global compliance
If you expand your enterprise outside the US borders, you may face data breach rules from other countries or regions your platform isn't designed to address, such as GDPR or Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

□ **The solution is regularly updated to reflect new and updated data privacy regulations that have a breach notification component.**
2 points

Proactive work missing
You have a solution that may not be keeping up with changes as fast as they occur. With more than 170 global privacy reporting regulations already in place and more being added every year, an oversight of any law can be costly to your business.

□ **The solution features a comprehensive, continuously updated database of breach notification regulations across all US states and many countries and industry-specific regulations that contain a privacy breach reporting requirement such as HIPAA.**
3 points

Ready when proposals become laws
This tool uses an internal team of certified privacy professionals to monitor and track the global regulatory landscape for upcoming and updated regulations. They update their database with any changes and inform you so you can review the relevance of the new laws and adjust your breach response plans as needed.

What process does your platform follow in responding to breaches?

3

□ **The platform notifies your privacy team members that a breach has occurred and that they may need to follow up with regulators in reporting the incident.**
1 point

Basic support
Regulations such as NYDFS have 72-hour deadlines for initial reporting to a regulator once a breach of personal data has been determined. Just knowing what supervisory authority to notify may not be enough for your team members. They need to know how to notify regulators and what to include in the notification to save time.

□ **The tool provides notifications on breaches for affected customers along with regulators.**
2 points

Don't assume you have all the information
Some regulations only apply in certain circumstances. If that information isn't automatically provided, then your team members may not know that they need it. Have your team get detailed instructions on what information must be included in with any consumer notification or guidance.

□ **The cybersecurity incident response process details the steps that the members of the privacy team should take to address the reporting requirements along with regulatory and consumer notifications.**
3 points

A detailed approach
With this feature, your tool can track data breaches that trigger multiple reporting requirements as separate tasks inside the overall incident. Privacy and security management officials can follow the same specific guidelines in responding to each incident. Users can assign specific users and specific timelines for incident tasks if desired as well.

How flexible is your tool in working with other services?

4

□ **The tool has a limited number of predefined integrations.**
1 point

Limited to no customization
This platform may not have all the capabilities you need as your business scales and expands current and future operations. Your workflow can potentially outgrow this tool, given the restrictive number of integrations.

□ **Third party integrations exist, but no customization.**
2 points

Only some potential explored
You may have a better range of security IT Ops and GRC available to integrate with your privacy breach reporting platform, but you are limited to vendor provided integrations. There are still customization restrictions for how your response processes meet your organizational processes.

□ **The solution allows for dozens of applications and can handle adding many new ones being developed.**
3 points

Prepared for many adaptations
A platform has an application store that allows you simple and easy access to published validated and community applications. You can also develop your own integrations for customized applications by using a fully documented Representational State Transfer application programming interface and developers' resources.

How does your tool handle breach risk assessments?

5

□ **The tool provides general instructions to guide your privacy team members through evaluating the risk of harm associated with a security incident.**
1 points

General assistance
This kind of breach risk assessment can have gaps in showing your team members what specific information they need to fill out for different kinds of assessments. What data NYDFS requests from your enterprise on breach risk can be different than what HIPAA seeks.

□ **Specific breach risk assessment templates are available for mandated regulations.**
2 point

Guided risk assessment
Regulations such as PIPEDA, GDPR and HIPAA have specific requirements and definitions of risk assessment. By providing specific templates for these regulations, the process of collecting the relevant information should be simplified.

□ **The platform has features allowing your privacy team to generate customized assessments for regulators.**
3 points

Customized reports
With this type of tool, your team members can create this report with just a few clicks on a keyboard. For example, one specific requirement of GDPR is that your privacy team needs to share documentation which demonstrates work has been done to ascertain the level of risk.

Does your tool offer incident simulation?

6

□ **No incident simulation feature is available.**
1 point

Separate method of simulation needed
To be cyber resilient, you should understand whether you have the right processes in place and if the right people have a clear understanding of their roles when a data breach occurs.

□ **Incident simulation is available, but there are a limited number of parameters that can be set in advance.**
2 points

Constraints on what you can test
Being limited in setting the scenario to test for your enterprise can make incident simulation frustrating. You should be able to determine the incident type, such as phishing or system intrusion; attack vectors such as email; the level of the severity of the simulation; name for future reference and review; and related criteria.

□ **The incident simulation helps security and privacy team members with alignment and incident response.**
3 points

An exercise that helps build teams and performance
This feature helps foster cohesion between your security and privacy team members as they simulate and prepare against a data breach incident. It also allows participants to repeat the process and offer feedback, bolstering your incident response plans and processes.

How does the tool handle reporting?

7

□ **The tool can generate simple, reconfigured reports based on common breach reporting requirements.**
1 point

Limited presentation options
A range of simple reports is a good start for sharing key metrics with a wider audience but can limit the overall reporting requirements that most organizations need.

□ **Fuller reporting options break down key performance indicators for different audiences.**
2 points

Security-only view
To gain visibility into your organization, it's helpful to break down security data from your dashboards and reports as much as possible. The ability to analyze the security data in your dashboards and reports helps you gain better insight into your organization and identify and target its data breach vulnerabilities.

□ **Extensive customizable dashboards and reports are available inside the tool and are exportable to wider reporting platforms.**
3 points

A fuller picture of your situation
These data summaries helps you to understand how effective your overall response process is for data breach reporting and related issues. By defining several criteria, you want to review, you and other executives can identify potential gaps in your data breach processes and areas where you might need additional resources. The ability to export key information into wider business reporting platforms improves the value of this information for your business.

Tally your score

Does your tool provide what you need?

□ Score: 7–12

A platform with minimal coverage
This platform may be missing features that could enhance your data breach and may not be able to meet your needs as your business scales, particularly with global expansion. You can encounter inconveniences in reviewing results and feel as if you are reacting to incidents too late.

□ Score: 13–18

A tool with capabilities but also limitations
While having more capabilities than the preceding options, you can notice the limitations. As new regulations and requirements to existing rules proliferate, you can potentially have more demands to monitor and address data breaches than this tool can adequately address in a timely manner.

□ Score: 19–21

A solution designed to meet your present and future needs
A solution can help you adapt to the changing regulatory landscape regarding incidents at your convenience. You can gain insights to help handle potential incidents for your enterprise. As a result, you can get more connectivity and coordination on handling data breaches between privacy and security team members, executives and customers.

Consider the criteria for security incident reporting
To meet evolving breach notification requirements, security teams should align with their privacy and legal colleagues. Security orchestration and automation technology can be an important tool in helping to enable this alignment. Current and upcoming regulations may require security teams to have a documented incident response plan and be able to execute the plan effectively and consistently. To help achieve these goals, privacy and security leaders should have the incident response process codified and orchestrated across their organizations, which can include tooling to help maintain a consistent, repeatable process for breach response. Consider these criteria for selecting a data breach notification tool:

- A single point of management for data breach preparation, assessment and management, tightly integrated with security operations for efficiency
- A regularly updated database of breach notification regulations across all US states and many countries and industry-specific regulations that contain a privacy breach reporting requirement
- An incident response process that details the steps that the members of the privacy team should take to address the reporting requirements along with regulatory and consumer notifications
- A setup that can add dozens of third-party applications and can handle adding new ones being developed
- Features that allow your privacy team to generate customized reports for regulators
- Incidence simulation that lets security and privacy team members become more aligned while being able to respond to real incidents
- Extensive dashboards and reporting available to all users

Take the next step
The privacy add-on solution from IBM® Security Resilient® is part of the wider Resilient Security Orchestration, Automation and Response (SOAR) Platform. This platform offers security and privacy teams intelligence and insights to help them respond to rapidly-evolving security incidents. The IBM Resilient SOAR Platform Privacy Add-On can help security and privacy teams understand and address complex regulatory requirements with speed and agility. To learn more about the IBM Resilient SOAR Platform and how it can help you, visit ibm.com/security/intelligent-orchestration/resilient/privacy-breach-preparation-response

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the GDPR readiness journey at IBM and GDPR capabilities and offerings to support your compliance journey at www.ibm/gdpr

[1] 1 The Fourth Annual Study on the Cyber Resilient Organization, independently conducted by the Ponemon Institute and sponsored by IBM Security, April 2019.

[2] GDPR, Article 33, http://www.privacy-regulation.eu/en/article-33-notification-of-apersonal-data-breach-to-the-supervisory-authority-GDPR.htm

[3] The Fourth Annual Study on the Cyber Resilient Organization, independently conducted by the Ponemon Institute and sponsored by IBM Security, April 2019.

[4] NYDFS, Section 500.16, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500sapa.pdf