resilient

Preparing for GDPR's Incident Response Challenges

Introduction

The European Union's General Data Protection Regulation (GDPR) goes into effect on May 25, 2018, and with it comes new challenges for organizations dealing with personal data and information loss of EU citizens. There are many complexities to how an organization will be required to respond to a data breach, and planning should start well in advance to ensure the incident response team is fully prepared before the GDPR mandate.

The Key Points of GDPR

- **72 Hours:** Any organization globally that collects personal data from EU citizens – whether the company is based in the EU or not – will have 72 hours to notify authorities of a breach
- **Notify Customers:** Organizations must notify their impacted customers "without undue delay" after becoming aware of the breach
- **Risk of Fines:** If your organization does not meet these requirements, you risk being fined €20m or up to four percent of annual revenues

Required Incident Response Plan

GDPR brings additional new requirements for individual companies beyond the timeline and penalties. Among the key mandates, companies that fall under GDPR will need an incident response plan and an audit of incident response activities. Each company will need to report these breach activities to a specific Data Protection Authority (DPA). Some companies may also need to appoint a Data Protection Officer (DPO) to supervise data collection.

For many companies, especially in the EU, this will be the first mandatory breach notification regulation they must follow. Preparation will continue to get more complex as the individual member states in the EU unveil their own laws in addition to the GDPR baseline. With the globalization of business today, many companies will need to adapt to account for customer breaches in different countries and work closely with the required DPAs and specific regulations in different countries.

THOUGHTS FROM THE EXPERTS:

"Only 25 percent of organizations say they have a cyber security incident response plan (CSIRP) that is applied consistently across the enterprise, despite the importance of having a CSIRP in place with skilled cyber-security professionals."

DR. LARRY PONEMON,
Chairman and Founder of the Ponemon Institute

According to IAPP, the number of DPOs required under the GDPR in Europe alone will be at least 28,000 – a number that is "conservative."

SOURCE: IAPP, 2016

What GDPR means for your Incident Response Team

With the new mandates under GDPR, incident response teams will have new challenges to face – and will need new and improved processes to satisfy the requirements and ensure compliance.

72-Hour Breach Notification Requirement

As mentioned, the most notable challenge will be the 72-hour data breach notification requirement. For IR teams facing this window, preparation is more important than ever. Responders will need clear and consistent processes to guide them through response and notification quickly and effectively.

Another complication from GDPR is that only certain data breaches need to be reported. For example, any breach that is more than the loss of personal data – or, more technically, if the breach could result in a risk to the rights and freedoms of individuals – needs to be reported. Gaining an innate knowledge of what to flag and when to flag will be necessary – and can best be learned and effectively addressed through simulations and practice well in advance of breaches.

> *"Most companies globally do not feel confident in their ability to comply with the upcoming requirements that GDPR will bring. Organizations should be proactive now, and establish processes and owners for ensuring GDPR compliance."*
>
> **DR. LARRY PONEMON,**
> Chairman and Founder of the Ponemon Institute

How an Orchestration Incident Response Program Helps with GDPR

To help overcome the uncertainty of the new regulations – such as what types of breaches need to be reported, when to report them, and who to report them to – an orchestrated incident response function can be effective.

Incident response orchestration aligns the people, process, and technology involved in incident response – empowering responders to triage and resolve incidents intelligently, quickly, and effectively. When faced with uncertainty, incident response orchestration is crucial to ensuring that the humans in the loop can address an incident on hand, decide what needs to be done, and take remedial actions quickly and accurately.

When managing a privacy breach, response involves more than the security team. Privacy, legal, marketing, and executives may all need to play a role. Incident response orchestration facilitates collaboration across the company — making your organization-wide compliance efforts more effective.

Speed and accuracy are critical given the new breach notification deadlines – and orchestrating the incident response and breach notification processes are key to meeting the tight deadlines imposed by GDPR. By automating the right technological processes to empower people in the process will help ensure the organization's response is efficient and accurate.

How IBM Resilient Empowers Compliant, Fast GDPR Breach Response

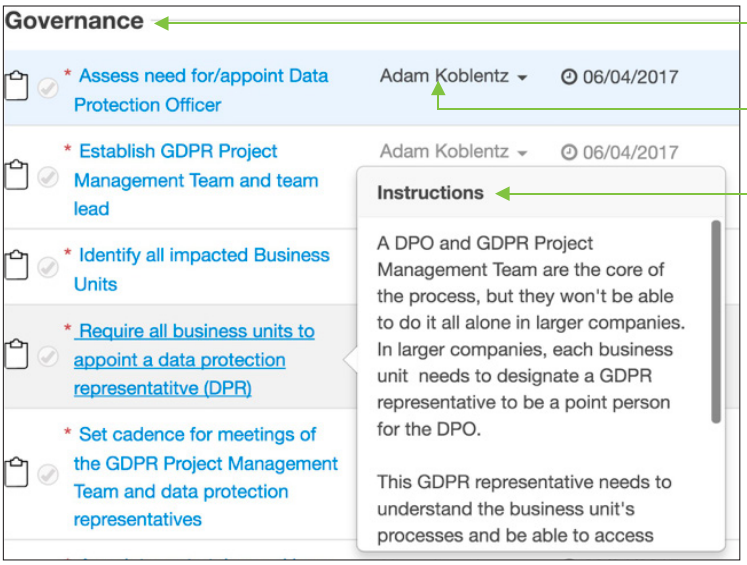
IBM Resilient has one of the world's largest breach notification databases integrated into our incident response platform, and provides detailed workflows for complying with specific regulations in the event of a breach. The Resilient Privacy Module, launched in 2011, supports more than 200 deployed customers who use the IBM Resilient platform to improve incident response and breach notification processes. We adapt daily to meet the changing regulations and the growing needs of our customers and prospects, including GDPR.

By leveraging the Resilient Incident Response Platform (IRP), customers will be better able to meet the new GDPR incident response regulations. Customers will be able to minimize the impact of GDPR on their business and reduce the risk of fines. The GDPR-enhanced Privacy Module provides customers with the information needed for reporting breaches under GDPR.

IBM Resilient Empowers Organizations to be Ready for GDPR

PREPARE

- **GDPR Preparatory Guide:** A documented, multi-step process stored within the platform.



Tasks are split into phases of preparation

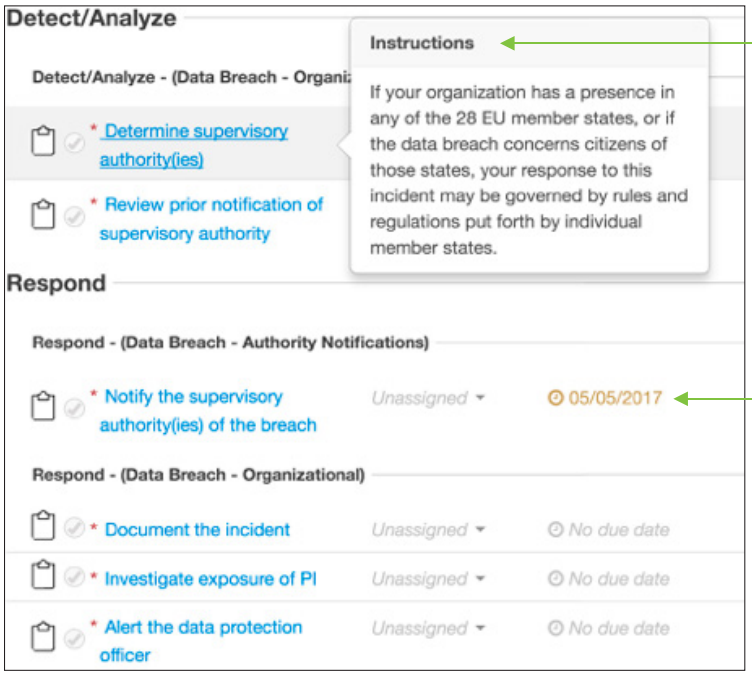
Tasks can be assigned to team members with due dates for easy tracking

Each task contains detailed instructions

The guide provides a set of tasks that can be added to the response workflow, assigned to others in the organization, and managed more effectively than via a static to-do list or spreadsheet. The Resilient GDPR Preparatory Guide provides a platform for which preparatory notes are stored within the platform, making it easier to track and document the GDPR preparation process.

PRACTICE

- **GDPR Simulation:** Security teams can rehearse their response to an incident under GDPR.



Analysts and privacy professionals can run tabletop games preparing for GDPR's breach notification requirements

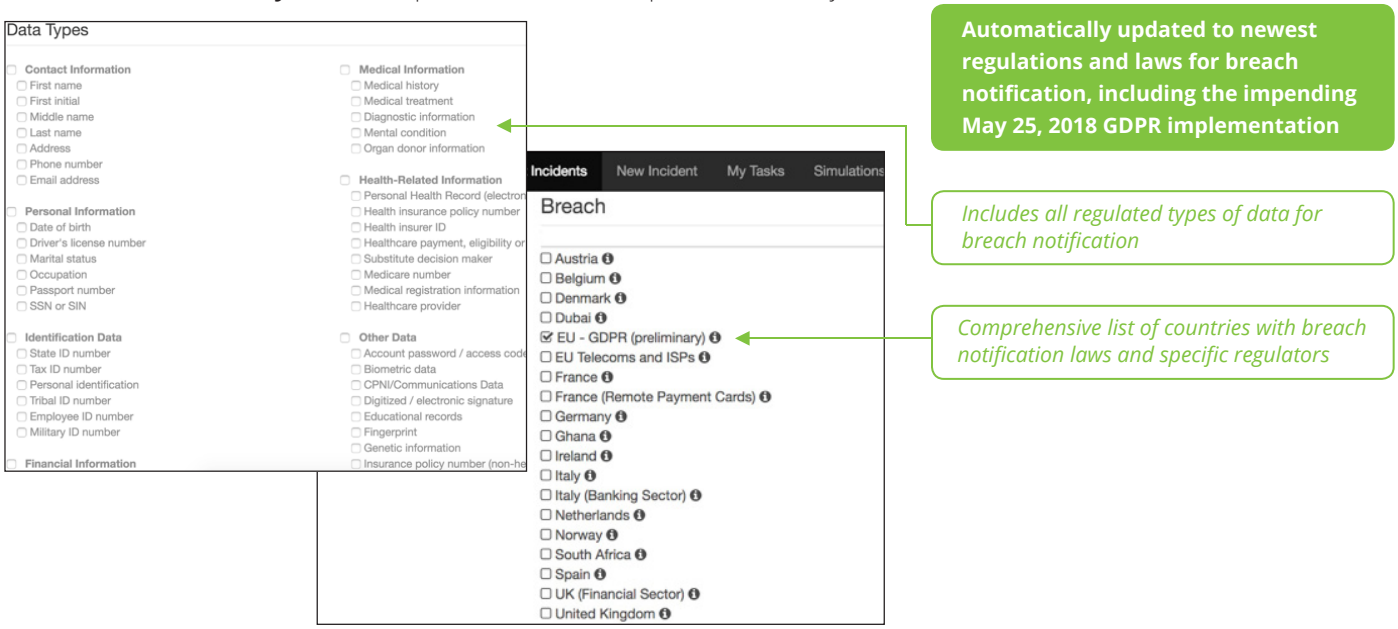
Every task has clear guidance instructions for the analyst

The new breach notification timeline is already set and counting down when a simulation is started

Simulating GDPR privacy breaches empowers organizations to proactively rehearse the actions they will have to take in the future, based on a breach under GDPR. It ensures both people and processes are battle-tested and well-practiced before a real data breach occurs.

RESPOND

- **GDPR-enhanced Privacy Module:** Updated with GDPR requirements in May 2018.



The Resilient Privacy Module guides organizations through the correct response to data loss incidents, helping to meet the regulatory deadlines and best practices for responding to an incident under GDPR. This gives privacy professionals the industry's only instant, highly customizable platform for breach preparation, assessment, and management. Once GDPR becomes enforceable on May 25, 2018, the Resilient IRP will empower organizations with the latest steps and requirements for breach notification based on your supervisory authority or authorities – built directly into your incident response plans.

With the Resilient Privacy Module, GDPR reporting requirements and security incidents can be completed in a fraction of the time of manual processes – and with greater confidence that your organization has followed the new regulations.

By leveraging adaptive response, the Resilient Privacy Module provides security teams with the speed, agility, and intelligence needed to contend with increasingly complex attacks.

Learn more about our offerings and best practices to prepare for GDPR at www.resilientsystems.com/our-platform/gdpr/

IBM Resilient's mission is to help organizations thrive in the face of any cyberattack or business crisis. The industry's leading Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has more than 150 global customers, including 50 of the Fortune 500, and hundreds of partners globally.

www.resilientsystems.com