GDPR and the Resilient Incident Response Platform

Data breach compliance in the European Union with IBM Resilient

Overview

The EU's General Data Protection Regulation (GDPR) goes into effect on May 25, 2018. The legislation in European data protection is significant as it will impact any organization that collects data from EU consumers. These organizations will have 72 hours to notify authorities of a breach, or risk being fined up to € 20 million or 4 percent of annual revenues.

IBM Resilient® arms organizations with the actions required under GDPR-related breach notification guidelines and laws incorporated into your incident response plans. This prescriptive guidance speeds response and provides a record of action.

Benefits

Leverage IBM Resilient to ensure your organization stays GDPR-compliant in the face of a breach.

Several articles of the GDPR cover the need for incident response and breach reporting. The Resilient Incident Response Platform (IRP) is uniquely qualified to help with these aspects of GDPR because it is based on a full orchestration platform for incident response. Orchestrating incident response enables companies to comply within a short notification period and provides guidance on how they should interact with the necessary authority.

IBM Resilient IRP offers:

- **GDPR Preparatory Guide:** An interactive tool that prescribes step-by-step how to prepare for GDPR. The guide leverages the flexibility of the Resilient IRP and makes preparation and planning interactive and dynamic. Tasks in the guide can be modified or assigned to more effectively manage the GDPR preparation workflow for the organization, beyond breach notification. The Resilient GDPR Preparatory Guide ensures that all aspects of the preparation are captured in detail, making it easier to track and document for the future.
- **GDPR Simulation:** This simulator within the Resilient IRP is where organizations rehearse the actions they will have to take in the future, based on a breach under GDPR. It walks analysts through the steps of assessing a risk and the necessary steps involved in reporting.
- **GDPR-Enhanced Privacy Module**: IBM Resilient is in the midst of a months-long effort to add GDPR regulations to its global privacy module. Once GDPR becomes enforceable on May 25, 2018, Resilient IRP will be armed with one of the world's most comprehensive databases of GDPR-related guidelines and laws embedded into an incident response platform.

The GDPR challenge

Organizations have 72 hours to notify authorities of a breach, or risk being fined up to 4 percent of annual revenues, and determining compliance is extremely complicated.

Companies may need to create and compete in the market for a new position: Data Protection Officer (DPO).
Current estimates put the need for DPO jobs at 75,000.

The promise of GDPR notification being a one-stop shop is unlikely.
The promise of harmonization from the regulation was going to come from a one-stop shop: an organization decides who their Data Protection Authority (DPA) is, and this person becomes the single person to whom they report any incidents. In reality, if an organization is diversified across the EU, the situation may be more complicated. and multiple DPAs may be involved.

Respond effectively with IBM Resilient.
Being prepared in advance of May 25, 2018 will help organizations reduce the risk of non-compliance and identify exposures and design processes. The IBM Resilient GDPR preparatory guide and world's first in-platform GDPR breach notification simulator will help get organizations prepared and practiced before GDPR goes into effect.

Preparing for GDPR with an orchestration model:

- **People**: Achieving and maintaining compliance with the GDPR will be an exercise in change management and will require dedicated leaders. Your company may even be required to appoint a DPO based on the type and volume of personal data you process.
- **Process**: In these early stages, privacy leaders should ensure they have a grasp on the fundamentals: What data does your organization hold? Where is it? Who has access? And how is it protected? You should document everything you uncover in this process. Companies should also ensure that there is internal alignment about compliance with notification. A company that might be tempted to not notify their supervisory authority about a breach should consider the risk involved with disgruntled employees becoming whistleblowers.
- **Technology**: Privacy and security leaders should examine if their tools provide compliance support—including if they enable documentation to demonstrate compliance, help manage and audit workflows, and properly arm you to fulfill your obligations.

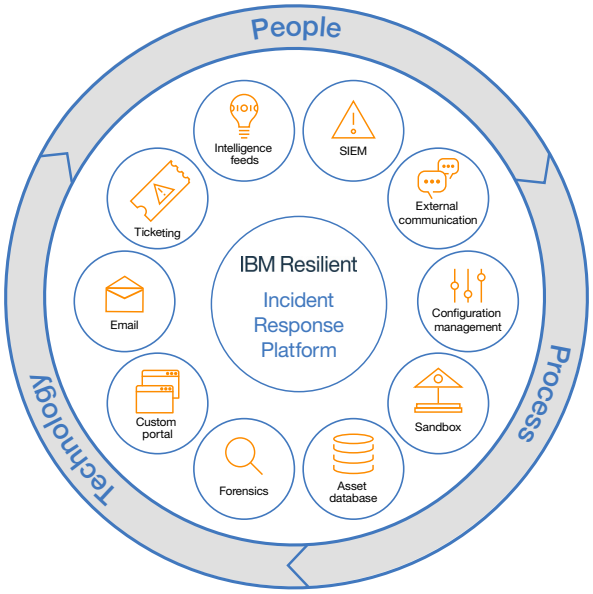

Figure 1: How the Resilient IRP acts as a central hub for IR orchestration

The Resilient IRP empowers organizations to thrive in the face of cyberattacks and business crises.

The Resilient Incident Response Platform (IRP) enables faster and more effective response through the orchestration and automation of IR processes. It works seamlessly with the prevention and detection systems you use today to create a central hub for IR management.

For more information on the IBM Resilient IRP, schedule a demonstration today: www.resilientsystems.com/demo

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

18013618USEN-00