IBM Security Launches New Capabilities to Help Clients with Impending EU General Data Protection Regulation

IBM Resilient Helps Clients to Rehearse, Prepare for and Manage GDPR

CAMBRIDGE, Mass., May 25, 2017 /PRNewswire/ -- IBM (NYSE:IBM) today announced new incident response capabilities, from its IBM Resilient security portfolio, to help companies address the new General Data Protection Regulation (GDPR). These capabilities are designed to help clients rehearse, prepare for and manage the new regulations. GDPR is one of the biggest changes in data privacy law in decades which goes into effect on May 25, 2018.

GDPR may require significant changes to the way organizations respond to consumer data breaches. For example, any organization that does business in Europe will have 72 hours to notify the supervising authority and data subject of a breach, or risk being fined €20 million or up to 4 percent of their global annual turnover. A recent Ponemon Institute study found that 75 percent of organizations admit they lack a formal cyber security incident response plan (CSIRP) applied consistently across the organization, meaning that GDPR response could prove to be challenging. [1]

IBM Security is launching new GDPR capabilities to its Resilient Incident Response platform (IRP) a year ahead of the 2018 deadline to give organizations time to begin preparing and adapting. New capabilities include:

- **Resilient GDPR Preparatory Guide**. An interactive tool that prescribes step by step how you can 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 covers all aspects of preparation and are captured in detail, making it easier to track and document for the future.
- **Resilient GDPR Simulation.** A new function within the Resilient IRP helps security analysts within an organization rehearse the actions they may need to take if they experience a breach under GDPR, such as practicing for the 72-hour breach requirement, assessing risk of harm, or communicating with the Data Protection Officer (DPO) and Data Protection Authority (DPA). As part of the simulation, analysts assess a risk as high, medium or low, and follow the steps of engaging with a DPA and notifying the consumers whose data was compromised. The Ponemon study also found that the top barrier to cyber resilience is insufficient planning and preparedness; GDPR simulations can help reduce this barrier.
- **Resilient GDPR-Enhanced Privacy Module.** IBM Security added GDPR regulations to its global privacy module and will continue to update it so that once GDPR becomes enforceable on May 25, 2018, IBM Resilient clients will have access to the database of GDPR-related guidelines and regulations embedded into an incident response platform. GDPR's extraterritorial provision means that non-EU-based companies that market to or process the information of EU Data Subjects are also affected. Despite this far-reaching impact, the Ponemon study shows that only about half of the 4,268 IT and IT security professionals surveyed have started to prepare for the GDPR regulation. [1]

"GDPR is ushering in some of the most important changes to European data privacy regulations in twenty years, much of it involving policies and documentation that are difficult to improve with technology," said IBM Resilient CEO John Bruce. "The Resilient Incident Response Platform is designed to help businesses comply with GDPR. It prescribes and can orchestrate people, process and technology in specific responses to data breaches."

Most organizations already struggle with responding to cyber incidents. According to another Ponemon study, 66 percent of the professionals surveyed say they are not confident in their organization's ability to recover from a cyber incident. Moreover, 41 percent say the time to resolve a cyber incident has increased in the past 12 months. [2]

"GDPR will add a new set of challenges for most organizations," said Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute. "Our research shows that most companies globally do not feel confident in their ability to comply with data

breach notification requirements. To get ahead of these challenges, organizations should be proactive about establishing processes and owners for ensuring compliance with the new requirements."

The GDPR-enhanced Privacy Module is designed to reduce the time and complexity of responding to a data breach under the new regulation. For example, a US-based company with customers in Europe and the US could experience a breach that affects customers in Germany and in Massachusetts, California, and New York. Without access to the Resilient IRP, the company would have to know what to do – and who to contact – to comply with GDPR for their German customers, as well as knowing the people and processes involved in complying with the relevant and varying US federal and state laws for MA, CA, and NY.

The Resilient IRP is part of the IBM Security immune system, which helps clients out smart threats by incorporating the very latest in cognitive, cloud and collaboration technologies.

View IBM Resilient's Responding to a Data Breach Post-GDPR Response Solution Brief and other GDPR assets on the IBM Resilient website, or learn more about IBM Security GDPR offeringshere.

About IBM Resilient
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 200 global customers, including 50 of the Fortune 500, and hundreds of partners globally. Learn more at **www.resilientsystems.com**.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

[1] Ponemon Institute and IBM Resilient, "The Cyber Resilient Organization" 2016

[2] Ponemon Institute and Citrix, "The Need for a New IT Security Architecture" 2017

Media Contacts:

John Pinkham, IBM Resilient
617-207-4160
john.pinkham@ibm.com

Sara Bosco, Ketchum
sara.bosco@ketchum.com
646-935-4366

SOURCE IBM