IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses

77 percent of firms surveyed lack proper incident response plans; while 69 percent report funding for cyber resiliency is insufficient

CAMBRIDGE, Mass., March 14, 2018 /PRNewswire/ -- IBM (NYSE:IBM) Security today announced the results of a global study exploring the factors and challenges of being a Cyber Resilient organization. The study was conducted by Ponemon Institute and sponsored by IBM Resilient and found that 77 percent of respondents admit they do not have a formal cyber security incident response plan (CSIRP) applied consistently across their organization. Nearly half of the 2800 respondents reported that their incident response plan is either informal/ad hoc or completely non-existent.

Despite this lack of formal planning, 72 percent of organizations report feeling more Cyber Resilient today than they were last year. Highly resilient organizations (61 percent) attribute their confidence to their ability to hire skilled personnel – but organizations need *both* technology and people to be Cyber Resilient. In fact, 60 percent of respondents consider a lack of investment in AI and machine learning as the biggest barrier to Cyber Resilience.

This confidence may be misplaced, with the analysis revealing that 57 percent of respondents said the time to resolve an incident has increased, while 65 percent reported the severity of the attacks has increased. These areas represent some of the key factors impacting overall cyber resiliency. These problems are further compounded by just 31 percent of those surveyed having an adequate Cyber Resilience budget in place and difficulty retaining and hiring IT Security professionals (77 percent).

"Organizations may be feeling more Cyber Resilient today, and the biggest reason why was hiring skilled personnel," said Ted Julian, VP of Product Management and Co-Founder, IBM Resilient. "Having the right staff in place is critical but arming them with the most modern tools to augment their work is equally as important. A response plan that orchestrates human intelligence with machine intelligence is the only way security teams are going to get ahead of the threat and improve overall Cyber Resilience."

The lack of a consistent CSIRP is a persistent trend each year despite a key finding from IBM's 2017 Cost of a Data Breach Study. The cost of a data breach was nearly $1 million lower on average when organizations were able to contain the breach in less than thirty days – highlighting the value and importance of having a strong CSIRP.

Conducted by the Ponemon Institute and sponsored by IBM Resilient, "The 2018 Cyber Resilient Organization" is the third annual benchmark study on Cyber Resilience – an organization's ability to maintain its core purpose and integrity in the face of cyberattacks. The global survey features insight from more than 2,800 security and IT professionals from around the world, including the United States, United Kingdom, France, Germany, Brazil, Asia-Pacific, Middle East, and Australia.

"A sharp focus in a few crucial areas can make a big difference when it comes to Cyber Resilience," said Dr. Larry Ponemon. "Ensuring the security function is equipped with a proper incident response plan, staffing, and budget will lead to a stronger security posture and better overall Cyber Resilience."

The executive summary of these findings can be downloaded here.

Other takeaways from the study include:

- **Staffing for Cyber Resilience-related activities is inadequate**
  - The second-biggest barrier to Cyber Resilience was having insufficient skilled personnel dedicated to cyber security.
  - 29 percent of respondents reported having ideal staffing to achieve Cyber Resilience.
  - 50 percent say their organization's current CISO or security leader has been in place for three years or less. Twenty-

three percent report they do not currently have a CISO or security leader.

- **Organizations are not ready for GDPR**
  - The General Data Protection Regulation (GDPR) takes effect inMay 2018 and will mandate that organizations have an incident response plan in place.
  - 77 percent of respondents do not have an incident response plan that is applied consistently across the entire enterprise.
  - Most countries surveyed do not report confidence in their ability to comply with GDPR.

Download Full Reports & Registers for the Webinar

To learn more about the full results of the study, download"The Third Annual Study on the Cyber Resilient Organization."

Sign up for our upcoming webinar:"Growing Your Organization's Cyber Resilience in 2018," which will be held onMarch 27, 2018 at 11:00 AM EDT.

About IBM Resilient
IBM Resilient is the industry's leader in helping organizations thrive in the face of any cyberattack or business crisis. IBM Resilient's proven 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, open incident response hub. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has 300 global customers, including 60 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 has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

CONTACT
Kelly Kane
IBM Security
413-297-2668
kkane@us.ibm.com

John Pinkham
IBM Resilient
617-528-1697
john.pinkham@ibm.com

SOURCE IBM