IBM and Ponemon Study Reveals Organizations Remain Unprepared to Respond to Cyberattacks
Wednesday, November 16, 2016 04:00:00 PM (GMT)

CAMBRIDGE, Mass., Nov. 16, 2016 /PRNewswire/ -- Resilient, an IBM Company (NYSE: IBM) and the Ponemon Institute unveiled the results of the annual Cyber Resilient Organization study, which found that only 32 percent of IT and security professionals say their organization has a high level of Cyber Resilience – down slightly from 35 percent in 2015. The 2016 study also found that 66 percent of respondents say their organization is not prepared to recover from cyberattacks.

For the second straight year, the study showed that challenges with incident response (IR) are hindering Cyber Resilience. Seventy-five percent of respondents admit they do not have a formal cyber security incident response plan (CSIRP) that is applied consistently across the organization. Of those with a CSIRP in place, 52 percent have either not reviewed or updated the plan since it was put in place, or have no set plan for doing so. Additionally, 41 percent say the time to resolve a cyber incident has increased in the past 12 months, compared to only 31 percent who say it has decreased.

"This year's Cyber Resilience study shows that organizations globally are still not prepared to manage and mitigate a cyberattack," said John Bruce, CEO and co-founder of Resilient, an IBM Company. "Security leaders can drive significant improvement by making incident response a top priority – focusing on planning, preparation, and intelligence."

According to respondents, an incident response platform (IRP) is among the most effective security technologies for helping organizations become Cyber Resilient, along with identity management and authentication, and intrusion detection and prevention systems.

The study also uncovered common barriers to Cyber Resilience. The majority – 66 percent – say "insufficient planning and preparedness" is the top barrier to Cyber Resilience. Respondents also indicate that the complexity of IT and businesses processes is increasing faster than their ability to prevent, detect, and respond to cyberattacks – leaving businesses vulnerable. This year, 46 percent of respondents say the "complexity of IT processes" is a significant barrier to achieving a high level of Cyber Resilience, up from 36 percent in 2015. Fifty-two percent say "complexity of business processes" is a significant barrier, up from 47 percent in 2015.

Conducted by the Ponemon Institute and sponsored by Resilient, *The 2016 Cyber Resilient Organization* is a 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 2,400 security and IT professionals from around the world, including the United States, United Kingdom, France, Germany, United Arab Emirates, Brazil, and Australia.

While a recent study from IBM's Institute of Business Value found that reducing incident response time is the top challenge facing security professionals today[1], this new survey from the Ponemon Institute shows that the majority of companies are still not taking the proper steps to plan an effective and comprehensive response plan.

While the results of the study show that many organizations have yet to implement effective planning and preparedness measures to respond to cyberattacks, studies show that incident response will become a greater priority within the next several years.[2]

"While companies are seeing the value of deploying an incident response plan, there is still a lag in having the appropriate people, processes, and technologies in place," said Dr. Larry Ponemon. "We are encouraged that this is becoming a more important part of an overall IT security strategy."

The executive summary of these findings and the infographic can be downloaded here.

Key takeaways from the study include:

- **Companies are experiencing frequent and successful cyberattacks**

    - More than half (53 percent) say they suffered at least one data breach in the past two years
    - 74 percent say they faced threats due to human error in the past year
    - When examining the past two years, 74 percent say they have been compromised by malware on a frequent basis, and 64 percent have been compromised by phishing on a frequent basis
- **Organizations can't maintain operations effectively or recover quickly post-attack**
    - 68 percent don't believe their organizations have the ability to remain resilient in the wake of a cyberattack
    - 66 percent aren't confident in their organization's ability to effectively recover from an attack
- **A lack of planning and preparation is the biggest barrier**
    - Only 25 percent have an incident response plan applied consistently across the organization. Twenty-three percent have no incident response plan at all
    - Only 14 percent test their incident response plans more than one time per year
    - 66 percent cite a lack of planning as their organization's biggest barrier to becoming resilient to cyberattacks
- **Ability to respond to a cyberattack has not improved significantly**
    - 48 percent say their organization's Cyber Resilience has either declined (4 percent) or not improved (44 percent) over the past 12 months
    - 41 percent say the time to resolve a cyber incident has increased or increased significantly, while only 31 percent say it has decreased or decreased significantly

About Resilient, an IBM Company
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, smarter and more efficiently. Part of IBM Security, the Resilient IRP also integrates security technologies into a single hub and provides an orchestrated workflow spanning an organization's people, process and technology driving down response time. With Resilient, security teams can have best-in-class response capabilities. Resilient has more than 130 global customers, including 30 of the Fortune 500 and partners in more than 20 countries. Learn more www.resilientsystems.com.

Journalists and bloggers can download b-roll and video about IBM Security X-Force Command Centers at:
http://ibm.newsmarket.com/Global/Latest-News/new-ibm-security-headquarters-in-cambridge-ma-with-industry-s-first-commercial-cyber-range/s/2f75af45-2dde-4777-872a-0b6197407a84

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 more than 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.

Media Contact:
Dan Kloeffler
Vice President, Senior Media Specialist, Ketchum
646-935-4036
dan.kloeffler@ketchum.com

[1] IBM Institute for Business Value, "Cybersecurity in the Cognitive Era: Priming Your Digital Immune System"

[2] IBM Institute for Business Value, "Cybersecurity in the Cognitive Era: Priming Your Digital Immune System"

Logo - http://photos.prnewswire.com/prnh/20090416/IBMLOGO

SOURCE IBM

Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US, 0FT60T-E