Bloomberg BNA

Privacy Law Watch™

VOL. 16, NO. 222 NOVEMBER 17, 2016

Cybersecurity

Most Organizations Around the World Are Unprepared to Respond to Cyberattack

Effective corporate resilience to cyberattacks is a learned art, so companies need to proactively prepare for them, cybersecurity professionals told Bloomberg BNA Nov. 16.

DataGravity Inc. Chief Information Security Officer Andrew Hay said ''too many companies are still waiting for a disaster to land at their doorsteps before they take action to protect their data.'' Organizations ''have yet to get adequately proactive about protecting their most impotant asset: their sensitive data,'' Hay told Bloomberg BNA.

Matt Rose, global director of Application Security Strategy at Checkmarx Ltd., an app security testing company, said ''the problem is that cyberattacks are not just a technology issue but a process and people issue as well.'' In order for security measures to work properly, ''people need to know how to use them and what to do to prevent a cyberattack in addition to responding to a cyberattack,'' Rose told Bloomberg BNA.

Doron Kolton, CEO and founder of TopSpin Security in Herzlyia, Israel, agreed. ''Careless employees are just as dangerous as rogue insiders,'' Kolton told Bloomberg BNA.

Hay added that reducing risks starts with data awareness. Companies can't lower their risk of being attacked until they know how exposed they are, he said. ''Data awareness also involves monitoring data activity levels and automating the alert mechanism for suspicious activities,'' Hay said.

According to a Nov. 16 study by Ponemon Institute LLC and Resilient Systems, Inc., approximately 66 percent of 2,000 information technology and security professionals surveyed said that their organizations aren't prepared to recover from a cyberattack. Furthermore, nearly a third of the respondents said that their organizations don't have a formal incident response plan.

International Business Machines Corp., which purchased Resilient Systems in February, also announced Nov. 16 that it will expand its incident response capabilities as a part of a $200 million investment. The expansion includes a global security headquarters in Massachusetts which the ''industry's first physical Cyber Range,'' where companies can experience getting ready for and responding to a cyberattack, using real malware and scenarios.

IBM is the 11th largest technology company in the world with a $150.87 billion market capitalization, Bloomberg data show.

Expertise Developed Over Time Cybersecurity incidents are common, the Ponemon-Resilient study found. More than half of the organizations surveyed in the study said that they experienced a data breach in the past two years, involving the loss of more than 1,000 records containing sensitive information. Such data breach incidents can be costly and time-consuming for organizations.

According to the Ponemon-Resilient Systems study, a data breach incident costs an average of $4 million and more than 70 percent of surveyed organizations reported that they spent the same or more time as last year dealing with a cybersecurity incident.

More than half of the respondents rated the value of ''cyber resiliency''—the capacity of organizations to maintain core purpose and integrity during cyberattacks—as essential to achieving strong security.

Ed Jennings, chief operating officer of Mimecast Co., which specializes in cloud-based e-mail management for Microsoft Corp. products, told Bloomberg BNA that ''when thinking about a cyber resilience strategy, it is important organizations aren't limiting themselves to just cyber defense.'' Simply planning for cyberattack prevention isn't enough he said. ''Security maturity varies extremely widely across organizations and industries'' and this is largely due to mindset as well as ''expertise sustained and developed over time,'' he said.

Ponemon-Resilient Systems study respondents said that insufficient planning was the top barrier to cyber resilience, followed by complexity of business, insufficient risk assessment, complexity of IT process and silos and company turf issues. The study ranked identity management, incidence response platform and intrusion detection as the top three security technologies to improve an organization's cyber resilience.

Kolton agreed that identity management is crucial. ''Although the dangers of weak passwords have been proven time and again, most companies do not enforce a password policy,'' he said.

By Jimmy H. Koo

To contact the reporter on this story: Jimmy H. Koo in Washington at jkoo@bna.com

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

 ISSN 0000-0000

The study ''The Cyber Resilient Organization: Learning to Thrive Against Threats'' is available for download at http://info.resilientsystems.com/ponemon-institute-study-the-cyber-resilient-organization.

  PRA ISSN 0000-0000