IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them
Thursday, April 11, 2019 10:00:00 AM (GMT)

Yet Use of Automation Improved Detection and Containment of Cyberattacks by nearly 25%

CAMBRIDGE, Mass., April 11, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the results of a global study exploring organizations' preparedness when it comes to withstanding and recovering from a cyberattack. The study, conducted by the Ponemon Institute on behalf of IBM, found that a vast majority of organizations surveyed are still unprepared to properly respond to cybersecurity incidents, with 77% of respondents indicating they do not have a cybersecurity incident response plan applied consistently across the enterprise.

While studies show that companies who can respond quickly and efficiently to contain a cyberattack within 30 days save over $1 million on the total cost of a data breach on average,[1] shortfalls in proper cybersecurity incident response planning have remained consistent over the past four years of the study. Of the organizations surveyed that do have a plan in place, more than half (54%) do not test their plans regularly, which can leave them less prepared to effectively manage the complex processes and coordination that must take place in the wake of an attack.

The difficulty cybersecurity teams are facing in implementing a cyber security incident response plan has also impacted businesses' compliance with the General Data Protection Regulation (GDPR). Nearly half of respondents (46%) say their organization has yet to realize full compliance with GDPR, even as the one-year anniversary of the legislation quickly approaches.

"Failing to plan is a plan to fail when it comes to responding to a cybersecurity incident. These plans need to be stress tested regularly and need full support from the board to invest in the necessary people, processes and technologies to sustain such a program," said Ted Julian, Vice President of Product Management and Co-Founder, IBM Resilient. "When proper planning is paired with investments in automation, we see companies able to save millions of dollars during a breach."

Other takeaways from the study include:

- **Automation in Response Still Emerging** – less than one-quarter of the respondents said their organization significantly uses automation technologies, such as identity management and authentication, incident response platforms and security information and event management (SIEM) tools, in their response process.
- **Skills Still not Paying the Bills** – only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience.
- **Privacy and Cybersecurity Tied at Hip** – 62% of respondents indicated that aligning privacy and cybersecurity roles is essential or very important to achieving cyber resilience within their organizations.

Automation Still Emerging
For the first time, this year's study measured the impact of automation on cyber resilience. In the context of this research, automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. These technologies depend upon artificial intelligence, machine learning, analytics and orchestration.

When asked if their organization leveraged automation, only 23% of respondents said they were significant users, whereas 77% reported their organizations only use automation moderately, insignificantly or not at all. Organizations with the extensive use of automation rate their ability to prevent (69% vs. 53%), detect (76% vs. 53%), respond (68% vs. 53%) and contain (74% vs. 49%) a cyberattack as higher than the overall sample of respondents.

According to the 2018 Cost of a Data Breach Study, the use of automation is a missed opportunity to

strengthen cyber resilience, as organizations that fully deployed security automation saved $1.5 million on the total cost of a data breach, contrasted with organizations that did not leverage automation and realized a much higher total cost of a data breach.

Skills Gap Still Impacting Cyber Resilience
The cybersecurity skills gap appears to be further undermining cyber resilience, as organizations reported that a lack of staffing hindered their ability to properly manage resources and needs. Survey participants stated they lack the headcount to properly maintain and test their incident response plans and are facing 10-20 open seats on cybersecurity teams. In fact, only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience. Furthermore, 75% of respondents rate their difficulty in hiring and retaining skilled cybersecurity personnel as moderately high to high.

Adding to the skills challenge, nearly half of respondents (48%) said their organization deploys too many separate security tools, ultimately increasing operational complexity and reducing visibility into overall security posture.

Privacy Growing as a Priority
Organizations are finally acknowledging that collaboration between privacy and cybersecurity teams can improve cyber resilience, with 62% indicating that aligning these teams is essential to achieving resilience. Most respondents believe the privacy role is becoming increasingly important, especially with the emergence of new regulations like GDPR and the California Consumer Privacy Act, and are prioritizing data protection when making IT buying decisions.

When asked what the top factor was in justifying cybersecurity spend, 56% of respondents said information loss or theft. This rings especially true as consumers are demanding businesses do more to actively protect their data. According to a recent survey by IBM, 78% of respondents say a company's ability to keep their data private is extremely important, and only 20% completely trust organizations they interact with to maintain the privacy of their data.

In addition, most respondents also reported having a privacy leader employed, with 73% stating they have a Chief Privacy Officer, further proving that data privacy has become a top priority in organizations.

About the Study
Conducted by the Ponemon Institute and sponsored by IBM Resilient, "The 2019 Cyber Resilient Organization" is the fourth 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 3,600 security and IT professionals from around the world, including the United States, Canada, United Kingdom, France, Germany, Brazil, Australia, Middle East and Asia Pacific.

To learn more about the full results of the study, download "The 2019 Study on the Cyber Resilient Organization."

Sign up for our upcoming webinar: "Leaders & Laggards: The latest findings from the Ponemon Institute's study on the Cyber Resilient Organization" which will be held April 30 from 12:00-1:00pm EST.

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 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please checkwww.ibm.com/security, follow@IBMSecurityon Twitter or visit the IBM Security Intelligenceblog.

Media Contact:
Cassy Lalan
IBM Security Media Relations
319-230-2232
cllalan@us.ibm.com

[1] Source: IBM/Ponemon Institute Cost of a Data Breach Study

View original content to download multimedia: http://www.prnewswire.com/news-releases/ibm-study-more-than-half-of-organizations-with-cybersecurity-incident-response-plans-fail-to-test-them-300830465.html

SOURCE IBM

Countries: Denmark, Finland, France, Germany, Netherlands, Sweden, United Kingdom, United States
Industries: Computer Electronics, Hardware & Software, High Tech Security, Peripherals
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US