Preparedness Pays Off: New Data Shows Breached Organizations Spend More Time, Money, and Effort on Cyber Resilience - And Reap the Benefits

September 10, 2024

Latest Commvault Research Reveals How Proactive Investments and Attention to Cyber Recovery Can Save Millions in the Event of a Breach

TINTON FALLS, N.J., Sept. 10, 2024 /PRNewswire/ -- Commvault, a leading provider of cyber resilience and data protection solutions for hybrid cloud organizations, today released new critical insights from its 2024 Cyber Recovery Readiness Report. This global survey of 1,000 security and IT professionals across 11 countries, reveals interesting behavior changes for organizations that have been breached versus those that have not.

The Commvault survey, done in collaboration with GigaOm, shows that organizations that have endured cyber incidents in the past don't want to get burned again. Consequently, they often reassess and invest in cyber resilience and recovery strategies in very meaningful ways. According to the survey:

- **Investments in cyber resilience increase:** Organizations that have been breached spend nearly 30% more on cybersecurity measures than those that haven't.
- **More attention is given to understanding data risk profiles:** Breached organizations are nearly 2.5 times more likely to prioritize understanding their data risk profiles, which highlight data types and relative levels of risk.
- **Cyber readiness testing is prioritized:** Breached organizations conduct more testing to find gaps in their cyber preparedness plans. Twenty percent of organizations that haven't been breached do not test their recovery plan at all, that number drops to just 2% for organizations that have been breached.

The impact of these added investments and focus on cyber resilience is significant. According to the survey, breached organizations that have invested in comprehensive cyber recovery plans recover 41% faster than their less-prepared counterparts. In terms of specific recovery times, breached organizations state that they are 32% more likely to recover within 48 hours compared to those that have not been breached – a much better outcome than the recovery times noted by other respondents, which could be three weeks or more. This reduced downtime can translate to significant savings, both in terms of direct financial losses and the preservation of customer trust and brand reputation.

"We've all heard the expression hindsight is 20/20, and that could not be more applicable when it comes to the findings of this survey," said Brian Brockway, Chief Technology Officer at Commvault. "Our survey shows that the most resilient organizations are those that continuously test and refine their recovery strategies, learning from each incident to strengthen their defenses. It's this proactive mindset, rather than reactive spending, that makes the difference."

Much like health insurance, where the cost of coverage often far outweighs the potential expenses of medical emergencies, cyber recovery readiness serves a similar purpose. The report underscores that the costs of being breached – ranging from operational disruption to regulatory fines – far exceed the expenses of proactive cyber resilience measures.

"The findings should be a call to action for all organizations, not just those that have been breached," said Chris Ray, Cybersecurity Analyst at GigaOm. "Cyber threats are constantly evolving, and so too must the strategies to counter them. It's about adopting a holistic approach to cyber resilience that integrates people, processes, and technology, ensuring readiness at every level."

In addition to these findings, Commvault and GigaOm were able to pinpoint five key capabilities, also called resiliency markers, that when deployed together, helped companies recover faster from cyberattacks and experience fewer breaches compared to companies that did not follow the same path. These five resiliency markers emerged after data analysis teams combed through the same survey results across a range of topics including: how often companies were breached, what resilience technologies were (or were not) deployed, and how rapidly businesses were able to recover data and resume normal operations. Read more on the five resiliency markers here.

More Information:

- Check out the full Cyber Recovery Readiness Report

- Join the Business Uninterrupted: Readiness Strategies from the Trenches of a Breach webinar | September 18, 2024 at 1:00 pm ET

Methodology
Commvault in conjunction with GigaOm conducted this inaugural study of 1,000 respondents across 11 countries in April 2024 to better understand their views on cyber readiness and how prepared their organizations are in the face of cyber threats. Respondents were from companies earning at least $10 million in annual revenues, with the majority earning $500 million or more. Thirty-five percent of respondents were board-level or C-Suite executives, 48% were senior-level management, and the remaining 17% were mid- or junior-level management. The 11 countries included in the survey are Australia, Canada, France, Germany, Italy, Japan, Netherlands, Spain, Sweden, United Kingdom, and United States.

About Commvault
Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organizations keep data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere—at the lowest TCO.

View original content to download multimedia:https://www.prnewswire.com/news-releases/preparedness-pays-off-new-data-shows-breached-organizations-spend-more-time-money-and-effort-on-cyber-resilience--and-reap-the-benefits-302242469.html

SOURCE COMMVAULT

Media Contact: Kevin Komiega, Commvault, 978-834-6898, kkomiega@commvault.com; Investor Relations Contact: Michael J. Melnyk, CFA, Commvault, 646-522-6160, mmelnyk@commvault.com