Cyber Insecurity: Report Finds Majority of Enterprises Expect an Imminent Cyber Attack

October 16, 2023 at 8:30 AM EDT

While boardroom alarms ring louder, the C-Suite's involvement in cyber preparedness is often still notably absent

TINTON FALLS, N.J., Oct. 16, 2023 /PRNewswire/ -- Commvault, a leading provider of data protection and cyber resilience solutions for hybrid cloud organizations, today released a new IDC report commissioned by Commvault entitled, "The Cyber-Resilient Organization: Maximum Preparedness with Bullet-Proof Recovery Survey."

In this report, IDC surveyed more than 500 security and IT operations leaders worldwide to get a current view of how organizations are perceiving modern security threats and approaching cyber resilience. Many of the key findings of this report can be broken down into three areas: C-level engagement in cyber preparedness initiatives; fears around data loss and vulnerable workloads; and the need for automation.

Cyber resilience starts in the C-suite – or does it?

The research shows that in many cases, senior executives/line-of-business leaders are minimally engaged in their company's cyber preparedness initiatives — only one-third (33%) of CEOs or managing directors and less than a quarter (21%) of other senior leaders are heavily involved. According to the research, the majority (52%) of senior leaders have no involvement in their company's cyber cases.

In addition to a lack of executive engagement, there is also often confusion between ITOps and SecOps teams in terms of who is doing what when it comes to cyber preparedness. Only 30% of SecOps teams fully understand ITOps' roles and responsibilities for cyber preparedness and response, and similarly, only 29% of ITOps teams fully understand what falls to SecOps.

According to IDC, business leaders need to play a key role in ensuring companies prioritize cyber preparedness. Additionally, organizations must ensure there is complete alignment between ITOps and SecOps teams as not doing so can make organizations more prone to successful attacks or lengthy recoveries.

Data loss is a big concern, and some workloads are more vulnerable than others

Sixty-one percent of respondents believe that data loss within the next 12 months is "likely" to "highly likely" to occur due to increasingly sophisticated attacks. Of the respondents surveyed, on-premises workloads were thought to be more vulnerable than cloud workloads. On a scale of 1-5, with 5 being highly vulnerable, respondents rated on-premises data repositories a 2.8 and physical workloads a 2.77 – higher than that of cloud workloads (2.67).

Data exfiltration remains the preferred tactic, and manual detection processes are falling short

The research also shows that data exfiltration attacks – when malware or a malicious actor carries out an unauthorized data transfer – occur almost 50% more often than encryption attacks, where hackers aim to decode encrypted data. Respondents ranked phishing as the most concerning threat to address, given that most ransomware attacks begin with a successful attack on user credentials.

Additionally, as cyber attackers deploy more clever tactics, relying on manual detection and reporting processes are very likely to result in missed anomalies and successful attacks. A potential solution – automation – could lead to faster detection to mitigate the intrusion impact. However, most organizations (57%) have limited automation for key functions, increasing their chances of missing a threat before it happens; only 22% report being fully automated.

"Cyber attackers never rest and are constantly discovering ways to exploit vulnerabilities. A truly effective cyber resilience strategy must go beyond just backup and recovery. It's crucial that organizations adopt a new approach that spans prevention, mitigation, and recovery," said Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC. "Whether on-premises, in the cloud, or in a hybrid environment, they must integrate multiple layers of defense. With AI now a tool for both defense and offense, the urgency for comprehensive cyber resilience has never been more evident."

"We are beyond just reacting to cyber threats. The C-suite must ensure teams are prioritizing proactive defense, real-time threat intelligence, and robust risk management to pave the way for genuine cyber resilience," said Javier Dominguez, CISO, Commvault. "It's also critical that SecOps and ITOps teams work closely together to look holistically at their security posture, end-to-end. With Commvault, resilience isn't an afterthought – it's the blueprint."

To review the full survey results, visit https://www.commvault.com/idc-whitepaper-the-cyber-resilient-organization.

Methodology

Commvault sought to learn how organizations are approaching cyber resilience, what gaps in cyber responses are common, and best-practices as learned and described by senior IT professionals. To facilitate this research, Commvault commissioned IDC to conduct an independent effort in finding answers to these important issues.

The research methodology used by IDC involved the most comprehensive methodology possible, involving all three primary research methodologies: focus group of eight IT leaders of major US companies (several multinationals) with CIO, CTO, and CISO titles; individual in-depth interviews of other CIOs; and a worldwide survey of senior IT and security professionals with an n = 513.

About Commvault

Commvault (NASDAQ: CVLT) is a global leader in cloud data protection. Our industry-leading platform redefines the next generation of data protection as the only solution with comprehensive data protection, proactive data defense, advanced ransomware protection, and a single view across all your data. This lets you secure, defend, and recover your data, applications, and production workloads – on-premises, in the cloud, over SaaS, or spread across hybrid and multi-cloud environments. The result is early warning of attacks, active defense to reduce the impact of intrusion, and rapid, accurate recovery of your data. Simply put, Commvault is data, protected. For over 25 years, more than 100,000 organizations have relied on Commvault to keep their data secure and ready to drive business growth. Learn more at www.commvault.com or follow us @Commvault.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cyber-insecurity-report-finds-majority-of-enterprises-expect-an-imminent-cyber-attack-301957114.html

SOURCE COMMVAULT

Media Contact: Kevin Komiega, Commvault, 978-834-6898, kkomiega@commvault.com; or Investor Relations Contact: Michael J. Melnyk, CFACommvault, 732-865-0458, mmelnyk@commvault.com