Bitglass reports 61% of companies had an insider attack in past year

Bitglass has released its 2020 insider threat report, which uncovers the state of enterprise security over insider threats. Enterprises report that the average cost of an insider attack is as much as $US2 million.

The report disclosed that employees, whether careless or malicious, can pose a great risk to organisations. A majority of survey respondents (61%) reported at least one insider attack over the past 12 months (22% reported at least six separate attacks).

Bitglass partnered with a leading cybersecurity community and surveyed IT professionals to understand how their businesses balance budgetary and data protection concerns while defending against insider threats.

Businesses are currently undergoing seismic shifts, including rapid migrations to the cloud and widespread adoptions of remote work and BYOD (bring your own device) policies. Along with these trends, securing against insider threats has become increasingly challenging.

Most organisations cannot guarantee that they can detect insider threats stemming from personal devices (82%) or the cloud (50%), while 81% find it difficult to assess the impact of insider attacks.

Despite these concerns, few respondents have a single platform that delivers complete, unified visibility and control for any interaction.

When dealing with multiple disjointed tools that provide disparate levels of protection, security professionals spend an inordinate amount of time managing each of the solutions individually.

As such, 49% of respondents stated that at least one week typically goes by before insider attacks are detected; additionally, 44% said that another week usually passes before the organisation recovers from the attacks.

While organisations were already working with constrained security budgets before the pandemic, security teams are now being asked to do even more with less. 73% of companies' security budgets are decreasing or staying flat over the next year.

"Enterprises report that loss of critical data and disruption to business operations are the biggest repercussions of insider attacks," said Anurag Kahol, CTO of Bitglass. "Along with brand damage, remediation costs, legal liabilities, and loss of revenue, these are serious ramifications that must be prevented. Enterprises need a multi-faceted security platform that is designed to monitor user behaviour, secure personal devices, deliver maximum uptime and cost savings, and prevent leakage on any interaction. Only then can they defend against insider threats."

To see all of Bitglass' findings, download the full report here:
https://pages.bitglass.com/CD-FY20Q3-Bitglass2020InsiderThreatReport_LP.html?&utm_source=pr

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au