INSIDER INTELLIGENCE | eMarketer

APR 07
Gadjo Sevilla

Study: One-third of US companies cover up cyber breaches and ransomware

Article

The news: Nearly half (42%) of IT professionals have been told to hush up data breaches and ransomware attacks, according to a survey by Bitdefender, per VentureBeat. More shockingly, **29.9% of respondents admitted to keeping a breach confidential** instead of reporting it.

Bitdefender surveyed more than 400 IT security professionals serving companies of over 1,000 employees.

Why it's worth watching: The trend of failing to disclose threats is escalating just as the cyberthreat landscape is becoming more aggressive, with **52% of organizations experiencing a data breach within the past 12 months**.

- Law enforcement agencies estimate the number of cybercrimes that go unreported by businesses in the millions, per CSO.
- A study by the Ponemon Institute found that **the average cost of a data breach is $3.86 million**.
- The five most common threats are software vulnerabilities and zero-days, phishing and social engineering, supply chain attacks, ransomware, and insider threats.

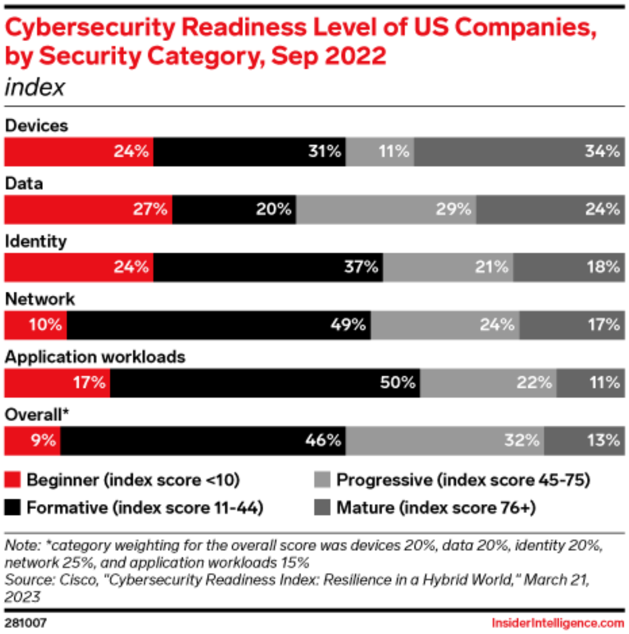
Why are businesses hiding security breaches? Organizations are burying data breaches to avoid legal and financial penalties or to skirt liability for compromising their user's data.

- The research comes less than a year after the FTC convicted former **Uber** CSO **Joseph Sullivan** for attempting to cover up a hack of Uber in 2016.
- In 2020, JBS was forced to pay $11 million to settle a class-action lawsuit brought by customers who were affected by a data breach that exposed their personal information.

The problem: According to the Annual Data Breach Report by the Identity Theft Resource Center, **41% of US companies have been breached multiple times in the past five years.**

- The consequences of being breached multiple times include financial losses and reputational damage, and some companies have even gone out of business as a result of ransomware.
- Rackspace laid off 275 employees last week, or 4% of its global workforce, due to an "uncertain macro environment." But this could be related to losses from its massive breach in December.

Key takeaway: The growing aggressiveness and sophistication of recent ransomware attacks reveals criminals repeatedly target businesses that don't report cyberattacks. Agencies are combating the threat, but more businesses need to report attacks.



Cybersecurity Readiness Level of US Companies, by Security Category, Sep 2022

index

*Note: *category weighting for the overall score was devices 20%, data 20%, identity 20%, network 25%, and application workloads 15%*
Source: Cisco, "Cybersecurity Readiness Index: Resilience in a Hybrid World," March 21, 2023

281007 InsiderIntelligence.com

This article originally appeared in Insider Intelligence's Connectivity & Tech Briefing—a daily recap of top stories reshaping the technology industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*