WINSTON & STRAWN LLP

BLOG

Data Report Finds Companies Need to Increase Focus on Data-Recovery Policies

JULY 31, 2018

Code42's recent 2018 Data Exposure Report, which featured responses from nearly 1,700 security, IT, and business leaders from the U.S., UK, and Germany, concluded, among other things, that "[w]hile companies know that prevention-only strategies don't work anymore, most haven't yet evolved to meet the new challenge."

The Report found that the threat of a data breach is significant; 61% of the CISOs and 53% of CEOs who responded said their companies have suffered from a data breach in the last 18 months. Additionally, 64% of CISOs and 56% of CEOs believed their company will experience a breach in the next 12 months that will go public.

While 84% of CEOs indicated that the seconds and minutes it takes to contain a breach may cost their companies money, 33% of security and IT respondents and 30% of business leaders said it would take up to one week to enact a business continuity plan to respond to a breach. 80% of CEOs and 72% of CISOs acknowledged that their companies need to improve their ability to recover from a breach. Moreover, 75% of CISOs and 74% of CEOs indicated their security strategies need to incorporate recovery-driven security, rather than just focus on prevention.

TIP: While companies should develop protocols and policies to help prevent a breach, they should assume a breach may occur and be well-prepared—before any breach—to quickly and sufficiently respond.

1 Min Read

Author

Steven Grimes

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

North America

Related Professionals

Steven Grimes

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.