CPA
Practice Advisor

FIRM MANAGEMENT

Business Leaders See Next Cyber Breach Coming from the Inside

71% worry about accidental internal staff error as one of the top threats facing their companies, almost on par with concern about outside hackers (75%).

David N. Plaskow • Feb. 13, 2023

While reports of professional cyberthieves breaching corporate and public sector servers dominate the news, a recent survey of business executives found that 71% worry about accidental internal staff error as one of the top threats facing their companies, almost on par with concern about outside hackers (75%). An additional 23% said they worry about malicious intent by an employee.

The survey, conducted by EisnerAmper's Outsourced IT Services practice during November 2022, found somewhat muted faith in current safety measures, with the largest share (51%) saying they are only "somewhat prepared," 39% feel "very prepared," 6% feel they are not at all prepared in their *overall* cyber defense strategies, and 4% are unsure. When asked about *internal* cyber defense, 57% are "somewhat confident," 37% are "very confident," and 6% are "not at all confident."

Training

The survey points to the need for ever-increasing vigilance via employee training and awareness, along with continued investment in system upgrades and staff. Only half (50%) said they are conducting cybersecurity training on a regular basis. A total of 44% held a training within the prior six months, 25% held a training more than seven months ago, and an alarming 31% said they had never held a single training event.

"A decade ago, business leaders likely equated cybersecurity breaches with external hackers, but the new normal of virtual and hybrid work has exposed a wide array of new cybersecurity threats, many coming from the inside," said Rahul Mahna, Partner and Head of Outsourced IT Services at EisnerAmper. "Businesses need to optimize their resources to ensure they are sparing no proactive measures. An important first step is training staff and refreshing that education at regular intervals. Given the increase in virtual/hybrid work, most companies should be conducting cybersecurity training at least quarterly. It's far more efficient to spend up front on education, state of the art software and hardware and, most of all, reliable IT staff who feel a stake in the company's success."

Budget

Seventy-one percent (71%) said they will keep their IT budget the same even during a recessionary economy, 21% said they will decrease their IT budgets, and only 8% expect to increase budgets.

The largest share of respondents (32%) said their annual spend on cybersecurity as a percentage of overall technology outlays was just 1%-3%, while 30% said that budget line was 4%-6%. Just 23% said the spending level was 10% or higher.

“This plays right into the hands of malicious actors,” noted Mahna. “When times are tough, these criminals expect companies to cut back, essentially leaving doors unlocked. In good times or bad, cybersecurity spending should always remain a top priority that yields significant return in losses avoided.”

Staffing

Businesses are not pulling back on IT staffing in the face of a looming recession, with only 5% of those surveyed saying they plan to reduce staff, while 24% plan increases. The largest share, 67%, said they will keep staffing the same, and 4% are unsure.

Firm Management • Hardware • Security • Small Business