EINPRESSWIRE

Enterprise Exposure to Cyberattacks Vastly Elevated with Increased Dependency on Third-Party Partners

Over half of survey respondents suffered an IT security incident in last two years due to flawed third-party software and services

NEW YORK, NY, UNITED STATES, February 2, 2023 /EINPresswire.com/ -- The pandemic rush to cloud computing proved costly for organizations who experienced a security incident stemming from vulnerabilities in their third-party relationships, according to new research from CyberRisk Alliance Business Intelligence, the research and content arm of cybersecurity data and insights company CyberRisk Alliance (CRA).

Sponsored by AuditBoard, the January Cybersecurity Buyer Intelligence Research report draws on responses from over 200 security and IT executives and leaders, security administrators, and compliance professionals across the United States. Many respondents indicated that their organizations' increased dependencies on vendors and other partners such as manufacturers, suppliers, and sub-contractors, as well as increasingly complex supply chains, have vastly elevated their exposure to attacks due to the lack of visibility into third and fourth-party partners (i.e., their vendors' partners) and the scope of data accessible to them.

"We use more third parties for services throughout the enterprise, and vulnerabilities for data, security and performance are even more visible and critical," said one survey respondent who cited the uncertainty around "downstream data processing in these third-party vendors."

Despite increased awareness and more demands to secure third parties, respondents stated that simply getting a third-party vendor or partner to implement good security controls can be a formidable challenge. When a third-party breach did occur, respondents said they didn't always receive timely notifications from their vendor or partner, limiting their ability to proactively notify customers and other stakeholders.

Organizations recognize that they must adopt a comprehensive risk appetite when they work with vendors and other partners and put greater pressure on third parties to respond to questionnaires about their security practices.

Key takeaways from the survey:

- Organizations are working with more third-party products and services than ever before, with an average of eighty eight (88) third-party partners (including software vendors, IT service providers, business partners, brokers, subcontractors, contract manufacturers, distributors, agents, and resellers). We expect this trend to continue in the next 12 months.

- More than half of all respondents (57%) reported they were victims of an IT security incident — either an attack or a breach — related to a third-party partner in the past 24 months. On average, organizations experienced two third-party related security incidents (attacks or breaches) in the past two years.

- About 80% of respondents experienced numerous consequences from these attacks, including network outages/downtime (31%), disruption in customer service (28%), business disruption or shutdown (27%), and 24% stolen/exfiltrated data (24%). One in five respondents reported financial losses or supply chain disruptions. Incidentally, 20% of respondents suffered financial loss. Nearly two out of three respondents (64%) reported some level of imposed costs and fees associated with their attack/breach. While 38% estimated their cumulative direct and indirect losses and costs — including legal fees, downtime, and loss of customers and business — were less than $100,000, another 26% said these costs exceeded $100,000.

- While organization size has no effect on the perceived importance of third-party risk management, the priority of these initiatives is highly correlated to the size of an organization. For example, about 6 out of 10 (59%) respondents from large enterprises specified third-party risk as either a critical or high priority at their organization, whereas smaller organizations are less likely to have this at the top of their priority lists.

- Overall, more than half (56%) said they expected “some investment” and 23% expected a “limited investment” in third-party risk management technology or resources in the next 12 months.

Some respondents noted plans to advance their third-party programs beyond the basics in the next 12 months, investing in human resources and technology to bolster their programs.

The full research report is available for download here.

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA’s brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

About AuditBoard
AuditBoard was born from a conviction that managing enterprise, assur¬ance, and compliance risk shouldn’t be manual, and that teams freed from administrative tasks can create more business value. That simple, yet powerful idea spurred the inception of our top-rated solutions and what’s now a modern connected risk platform. AuditBoard is leading a movement transforming risk professions, closing resiliency gaps, and elevating audit, risk, and compliance teams to a more strategic position of influence within their organizations.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here
Visit us on social media:
Twitter
LinkedIn