CyberRisk Alliance Releases 2022 Cybersecurity Year in Review Report

Cyberattacks increased and the post-pandemic world presented many challenges, but emerging technologies and solutions help security teams fight back

NEW YORK, NY, UNITED STATES, December 14, 2022 / EINPresswire.com/ -- CyberRisk Alliance Business Intelligence (CRA BI), the research and content arm of the data and insights company CyberRisk Alliance, released its "2022 Cybersecurity Year in Review: Everything, Everywhere, All at Once" report which highlights seven key areas where cybersecurity practitioners faced significant challenges but, in many cases, were able to make progress thanks to emerging technologies and fresh approaches to problem solving.

The report is a mix of original analysis and executive summary of significant findings from multiple in-depth surveys conducted throughout the year by CRA's research team on cloud security, zero trust, endpoint security, extended detection and response (XDR), vulnerability management, email security and threat intelligence. On average each individual survey gathered feedback from up to 300 security practitioners from across the United States, creating a powerful in-depth look at these important topics from a practitioner perspective as it evolved throughout the year, thereby allowing the CRA BI research team to identify key trends in the research and map it to the present state of cybersecurity at the end of 2022 and into 2023.

"In 2020, the world panicked, then pivoted to survive. Digital transformation accelerated and expectations evolved as did threats targeting organizations still transitioning to a new way of working. In 2022, organizations suffered the headaches that come with this new world and struggled to find the way forward," said Bill Brenner, VP of Content Strategy. "But with tools and frameworks like zero trust, XDR and more automated threat intelligence tech to bolster vulnerability management, cloud, email and endpoint security, organizations fought back – and established plans to invest more to secure networks and data in the next two years."

Key findings from the seven areas include:

- Cloud security: Cloud Security Alliance (CSA) researchers reported that only 39% of

organizations surveyed said they had high levels of confidence in their ability to secure cloud data, while only 4% reported sufficient security for 100% of their data in the cloud. The survey also found that third parties, contractors, and suppliers are the most commonly targeted groups (58%) in cyberattacks. And approximately 92% that have already experienced a data breach believe they will experience another breach of cloud data in the next 12 months.

• Zero trust: Zero trust gridlock contributed to slow adoption with only one out of four respondents reporting their organization had implemented zero trust. Those who hadn't made the leap to zero trust in 2022 said the transition was just too difficult and wouldn't be effective for their organization. Others said budget limitations and inadequate staff to provide oversight or support for a zero-trust model kept them from adopting it. The most prevalent obstacles to adopting zero trust, however, were the lack of knowledge about the framework and lack of buy-in from senior management.

• Endpoint security: As the number of endpoints continued to expand, the CRA survey respondents did their best to keep up. In addition to monitoring traditional devices like PCs and servers, a large majority (84%) reported they also monitor mobile devices on their network, with respondents reporting that their security solutions cover large volumes of both traditional and non-traditional endpoints and devices. Nearly two-thirds (63%) of respondents said they are managing more than 1,000 traditional and non-traditional devices.

• XDR: While familiarity with XDR is high (70%), current adoption of an XDR platform is relatively low; only 12% of respondents reported using this technology. But for those either using the technology or planning to invest in it, top benefits include faster detection and overall risk management improvement.

• Vulnerability management: Underscoring their focus on vulnerability prioritization, CRA survey respondents addressed the more exploitable vulnerabilities of their higher-value assets. And in many instances, increased budgets, resources, and staff allocations were put in place to bolster security programs. More than two-thirds, (69%) of respondents, said their budget or spending on vulnerability management would increase in the next 12 months, especially for things like automation.

• Email security: Due to a significant and steady number of email attacks, one-third of CRA respondents experienced up to 25 attacks daily. Additionally, about half (51%) of all respondents reported up to 25 business email compromise (BEC) attacks per day while 1 in 5 (21%) said they didn't know and couldn't estimate the volume of daily BEC attacks. At least half the respondents (51%) said they were very or extremely concerned about email attacks in the next 12 months. The threat of a ransomware attack was a top email security concern for two-thirds of all respondents, followed by an increase in spoofing and phishing.

• Threat intelligence: Emerging as a useful tool for educating executives, many also credit threat intelligence for helping them protect their company and customer data — and potentially saving

their organization's reputation, with top use cases for threat intelligence being vulnerability management (68%), security operations (66%), and incident response (62%). Technical (73%) and operational (71%) threat intelligence are more common than the more difficult strategic or more basic tactical use cases. Only 5% said they did not use any threat intelligence.

While each of the seven chapters in the report addresses specific concerns related to the cybersecurity area, a consistent theme permeating every survey centered around budgets, with one respondent stating it best: "Budget is always a hot topic and never really gets better. Trying to get the organization to be adaptable to new threats and to be prepared is always challenging."

The full 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. Learn more.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here