FOR IMMEDIATE RELEASE

Contact: Jenn Jones
Phone: (857) 328-0173
Email: press@cyberriskalliance.com

CRA Study: Managing Third-Party Risk in the Era of Zero Trust

New York, NY, March 23, 2022 – Companies large and small are struggling to stave off data breaches and prevent compliance violations as third-party partners they increasingly rely upon come under attack. These findings are according to a new survey fielded by CRA Business Intelligence, the insights and research unit of cybersecurity information services company CyberRisk Alliance, and SecurityScorecard, the global leader in cybersecurity ratings.

The survey, underwritten by SecurityScorecard, gauged how well organizations understand and manage risks associated with third-party relationships. Conducted from October through mid-November 2021, 250 U.S.-based IT and cybersecurity decision-makers and influencers participated.

Public and private sector organizations grant multiple third parties access to their private networks and sensitive databases, and they rely on them for everything from expense reporting and email services to managing industrial control systems. More than one-third of participants in this study had at least 100 third-party relationships, with some sectors, such as healthcare and government, working with 500 or more vendors at any given time.

Each vendor has the potential to create additional vulnerabilities by expanding the number of entry points into an organization's digital footprint. Yet most organizations lack the continuous visibility and knowledge of the security risks these third-party networks present. As a result, 91% of respondents had experienced a security incident related to a third-party and expressed some level of concern with experiencing another breach or falling out of compliance due to a partner vulnerability during the past 12 months.

While nearly one-third of participants are very interested in adding technology solutions to their risk management programs – principally to improve remediation times, risk assessments and regulatory compliance stances - priorities for managing third-party risk vary by industry. For instance, regulatory compliance is a top priority for healthcare, while risk assessment is a priority for financial services. Insurers seek more collaboration from their partners, while government organizations at the state, federal and local levels are looking for improved response and remediation times.

Among the study's key findings:

- Ninety-five percent (95%) of respondents expressed some level of concern with IT security risks from third-party business relationships, and 67% of participants experienced a significant increase in third-party-related security events within their organizations during the past year.
- Those working in the heavily regulated financial services sector were most apt to report a third-party-related cyber event.
- The most popular mitigation strategy for managing third-party IT security risks was a hybrid approach in which some, but not all, work is completed in-house.
- A majority of those surveyed were at least considering – if not already incorporating – principles of zero trust to reorganize privileges and restrict third-party user and device access to their networks.

"SecurityScorecard is proud to partner with CyberRisk Alliance to uncover insights into how organizations of all sizes are managing third-party vulnerabilities as a primary vector for malicious cyber attacks," said Aleksandr Yampolskiy, Co-Founder and CEO of SecurityScorecard. "Organizations must account for continuous visibility and monitoring of third-party networks as they move closer to a zero trust approach to cybersecurity."

"The report's findings highlight why organizations must have a comprehensive view of their cyber ecosystem not just to protect themselves, but also to determine if their vendors are well protected. Every organization is only as strong as its most vulnerable third-party," explains Matt Alderman, EVP, Foresight at CyberRisk Alliance.

The full research report is available for download here.

Join SecurityScorecard CISO Mike Wilkes on April 19th at 2 PM ET, for a live webcast to discuss the survey results and examine the pros and cons of incorporating automation into the various elements of third-party risk management.

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, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now Identiverse, ChannelE2E and MSSP Alert. Click here to learn more.

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

###