**For Immediate Release**

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

# CRA Research: A Turbulent Outlook on Third-Party Risk

**Companies have little visibility into the security of the third parties they use**

**New York, NY, February 8, 2022 –** Third-party relationships have expanded exponentially as companies seek outsourced services and software to perform optimally and backfill talent amid the ongoing pandemic. That expansion has broadened attack surfaces as threat actors target weaker vendors with strong market penetration to quietly surveil and paralyze systems.

For security teams trying to track the security practices of those third parties, visibility is essential but painfully limited, according to a new survey from CRA Business Intelligence, the research and content arm of cybersecurity information services company CyberRisk Alliance.

The survey was conducted in late fall 2021 among more than 300 IT and cybersecurity decision-makers and influencers who use third parties. Survey objectives were to gauge how well organizations understand and manage risks associated with third-party partnerships. Study participants were asked about their own vendor relations, concerns, and challenges in managing certain risks, and the impact of IT security incidents related to their third-party partners. They also provided responses to structured survey questions and were encouraged to provide corresponding comments where applicable. The study was sponsored by Detectify, Process Unity, OneTrust, Interos, Metric Stream and Trava.

Among the study's key findings:

- Sixty percent of respondents experienced an IT security incident in the past two years due to a third-party partner with access privileges and were most likely to have sensitive data stolen or suffered some type of business outage.
- While 52% of those who experienced third-party related attacks indicated they lost less than $100,000 in damages, another 45% incurred higher costs, with a few paying $1 million or more.
- Supply chain visibility is more essential than prior to the pandemic. Almost everyone wanted this ability, with 72% believing that tracking components, sub-assemblies, and final products was very or critically important. But respondents lamented that such visibility is severely limited.
- More than three out of four (76%) IT leaders and influencers rated managing third-party risk as a high or critical priority at their organizations—for most respondents (74%) this priority has increased in importance since 2020, when the pandemic created major micro and macro business disruptions, including supply and workforce shortages.

"Having started my compliance career in third-party vendor management in 2003, I'm still surprised at the lack of visibility into the risk that third-party suppliers pose to organizations," said Matt Alderman, EVP of CyberRisk Alliance's Business Intelligence Unit. "This research confirms that third-party risk is a critical component of your overall risk management program, especially considering recent attacks. With increasing damages and outages, it's time for organizations to manage the risk of their third-party suppliers."

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, 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. More information is available at http://cyberriskalliance.com/.

###