For Immediate Release

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

CRA Ransomware Study: Invest Now or Pay Later

Many victims are paying ransom, and despite efforts to bolster defenses, many continue to struggle with detection and response

New York, NY, February 24, 2022 – Ransomware attacks continue at a blistering pace because organizations remain vulnerable to the exploits bad actors use. Many victims are paying ransom, and despite efforts to bolster defenses, many continue to struggle at detection and response. Those are among the findings in a new survey report from CRA Business Intelligence, the research and content arm of cybersecurity information services company CyberRisk Alliance.

The data and insights in this report are based on a survey conducted in January 2022 among 300 IT and cybersecurity decision-makers and influencers. All were in the United States except for 1% from Canada, with respondents drawn from organizations of all sizes and industries. The study was sponsored by Attivo, eSentire and Menlo Security.

Among the study's key findings:

- Forty-three percent (43%) of respondents suffered at least one ransomware attack during the past two years. Among them, 58% paid a ransom, 29% found their stolen data on the dark web, and 44% suffered financial losses.
- Thirty-seven percent (37%) said they lack an adequate security budget, while 32% believe they're powerless to prevent ransomware attacks because threat actors are too well-funded and sophisticated.
- Remote workers and cloud platforms/apps were the three most common attack vectors:
    - Remote worker endpoint (36%)
    - Cloud infrastructure/platform (35%)

    - Cloud app (SaaS) (32%)
    - Trusted third-party (25%)
    - DNS (25%)
    - Software supply chain provider/vendor (24%)
- Exploitable vulnerabilities accounted for the most common initial infection point (63%), followed by privilege escalation (33%), credential exfiltration (32%), and averse mapped shares (27%).
- Respondents are most concerned about losing access to their organization's sensitive data (70%); stolen data being sold on the dark web (58%); ransomware gangs gaining privileged access and/or controlling directory services (53%).
- Companies are not taking the threat lying down: 62% will increase ransomware protection spending.

Attackers are gaining entry through current work and cloud computing configurations. Thirty-five percent (35%) of respondents report that ransomware attacks exploited remote workers. Among the various vectors were cloud infrastructure and platform services (35%), and cloud applications (32%). Other methods, such as DNS, software supply chain, third-party partners, and on-premises endpoints were also mentioned.

"2021 gave witness to elevated levels of ransomware attacks, and there is no reason to believe 2022 will be different," said Matt Alderman, EVP of CyberRisk Alliance's Business Intelligence Unit. "Our research confirms ransomware is still a big problem and cyber insurance is not the answer. On average, organizations will invest 4 – 5% more in 2022 to address ransomware in 2022. But it takes time to implement these solutions, leaving most organizations vulnerable well into the new year."

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. Visit the CyberRisk Alliance website to learn more.

###