

CRA Study: Zero Trust - Two Steps Forward, One Step Back

Efforts to implement zero trust are hobbled by concerns about user experience and business impact

NEW YORK, NY, UNITED STATES, March 29, 2023 /EINPresswire.com/ -- Zero trust is now a top priority for most organizations, but new research from CyberRisk Alliance Business

Intelligence, the research and content arm of cybersecurity data and insights company [CyberRisk Alliance \(CRA\)](#), shows efforts to deploy the framework facing headwinds – specifically over concerns about the user experience and impact on the business. Of the 200+ security and IT leaders and executives, practitioners, and compliance professionals surveyed, nearly 25 percent of those who have partially or fully implemented zero trust say they struggle to get full buy-in from other departments when it comes to scaling these ideas across the enterprise due to configuration issues (e.g., legacy apps that don't interact well with zero-trust technology).

As one respondent put it, “completely transforming the technology infrastructure takes time. Even if an organization has a sound architecture model and support from the business, executing is what matters — and those that don't execute accordingly will never meet the intentions of zero trust in the first place.”

Another respondent said, “Zero trust addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.” But according to another respondent, “It's difficult to find human resources with zero-trust skills, and we don't have supporting infrastructure and appropriate identity and access management (IAM) tools to enforce the zero-trust framework.” Despite its perceived importance, “getting upper management to completely sign off on the need for zero trust is also a challenge.”

Key takeaways:

- Only 24% of respondents have partially or fully implemented zero trust. Respondents say they continue to struggle with understanding the principals and configuration of zero trust.
- Nearly two-thirds of future zero trust adopters expect to have moderate difficulty in



implementing it. Another 30% expect high difficulty. Pain points: ensuring it meets business needs, plays well with legacy apps and doesn't disrupt user experience.

- Of those who are more advanced in their zero-trust implementation, 69% are motivated by pressure to close data security holes. MFA, IAM and least privilege access are the most common components of zero-trust strategies and implementations. Only one-third have formal zero trust policies.
- Zero trust marks a monumental shift in philosophy/practice. Respondents describe it as a "dramatic paradigm shift in security philosophy" that will require strategically reassessing how to secure the entire infrastructure to address challenges of remote or hybrid offices, multi-cloud environments, identity and authentication, and rapidly expanding endpoints.

In addition to survey insights, the report offers guidance to inspire organizations to pursue zero trust with greater awareness around implementation. For more detailed findings and analysis, 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](#).

Jenn Jones

CyberRisk Alliance

+1 857-328-0173

[email us here](#)

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/624817508>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.