EINPRESSWIRE

CRA Study: Remote Workers Spell Trouble for InfoSec

Attackers have capitalized on security vulnerabilities with employees working outside company walls

NEW YORK, NEW YORK, UNITED STATES, June 1, 2022 /EINPresswire.com/ -- As Enterprises and government agencies across the globe rush to support employees working remotely during the pandemic, attackers seized upon the resulting vulnerabilities, leaving security teams stretched thinly and struggling to keep up, according to a new survey from CRA Business Intelligence, the research arm of cybersecurity information services company CyberRisk Alliance.

The data and insights in this report are based on an online survey conducted in early 2022 with 1,100 IT and cybersecurity decision-makers and influencers representing 11 countries. Participants ranged from chief executives to senior analysts or their equivalents across several continents. Roughly 100 participants were selected from each of the following countries: United States, Mexico, Brazil, United Kingdom, Germany, France, The Netherlands, Spain, United Arab Emirates, Australia, and Singapore.

The survey was underwritten by global IT automation and security provider Infoblox, whose products, platforms and network services focus on DNS, DHCP and IP address management as well as cloud and virtualization.

Among the key findings:

• The surge in remote workers and highly distributed customer bases has changed the corporate landscape significantly – and permanently.
While some companies report they have shuttered physical offices for good, others still holding on to commercial properties must contend with remote staff or hybrid workplaces for the foreseeable future. As a result, some (%) moved more applications into the cloud and now rely on traditional network security staples such as VPNs and firewalls placed on corporate mobile devices. For employees using their own equipment, many companies are deploying solutions to

monitor and manage DNS, DHCP and IP traffic moving in and out of servers.

- The new workforce reality elevates concerns with data leakage, ransomware and attacks through remote access tools and cloud services. Respondents indicated concerns about their abilities to counter increasingly sophisticated cyberattacks with limited control over employees and vulnerable third-party partners. The sophistication of state-sponsored malware also is a source of worry for many.
- Organizations have good reason to worry: Most participants experienced up to five security incidents leading to at least one breach.

Attacks tended to originate with WiFi access points, employee-owned endpoints, or the cloud. Phishing was a common conduit to gain illegal entry to hijack credentials and steal or lock down data files. These weren't minor events either; the study showed 40% suffered at least US $1 million in direct and indirect losses.

- Interest in Secure Access Service Edge (SASE) frameworks is accelerating. As assets, access and security move out of the network core to the edge with the push for virtualization, 53% have already partially or fully implemented SASE and another 28% intend to do so.
- IT security budgets and spending increased for many in 2021, with even more security teams expecting a bump in budgets in 2022.

Many are considering primarily hybrid-oriented solutions that protect assets both on premises and in the cloud. And they are trying a wide variety of solutions – everything from end point and network security to cloud access security brokers, DNS security and threat intelligence services.

"Lots of organizations (52%) accelerated digital transformation efforts to support remote workers, while others (42%) increased support for remote customer engagement, but at what cost?" asks Matt Alderman, EVP at CyberRisk Alliance. "Our research highlights the extreme elevation of security risks associated with remote workers, remote networks, and cloud services, including ransomware and data leakage. To keep up, most organizations (72%) will increase spending in 2022 on a wide variety of endpoint and network security solutions, including SASE, to reduce the risk of remote workers. It's taken us two years to get to this point and it will take us at least two years to mitigate all the risk."

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, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. Click here to learn more.

About Infoblox

Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70% of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. Learn more at https://www.infoblox.com.

Jenn Jones
CyberRisk Alliance
6178338853 ext.
press@cyberriskalliance.com