

Asset Visibility is Top Challenge for Security Professionals

Survey of security professionals shows that asset visibility, staffing, and compliance with industry regulations were the biggest challenges facing the industry

LONDON, UK, July 12, 2022

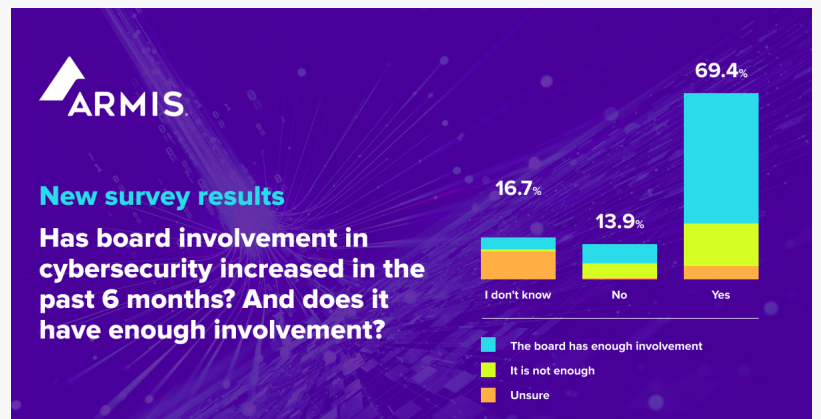
/EINPresswire.com/ -- [Armis](#), the leading unified asset intelligence platform, surveyed over 100 security professionals in response to the growing number of ransomware and cyberattacks across the globe. The survey aimed to explore the major challenges, risks, and worries of business leaders in the cybersecurity industry. Top industry risks were found to be employee behaviour, poor [asset visibility](#), and poor patch management practices.

After years of fighting for airtime at the top, almost seven in ten respondents claimed that board involvement in cybersecurity has increased within the past six months. Though encouraging, nearly a quarter (23%) of respondents thought that board members still do not have enough involvement with cybersecurity.

Results indicate that the top 5 priorities for cybersecurity are risk assessment, [compliance](#), asset visibility, security



Industry challenges and risks



Board involvement in cybersecurity



Top priorities in cybersecurity

awareness training, and threat detection/incident response. Furthermore, organisations have begun modifying their responses to cybersecurity concerns over the last six months, with a third saying their businesses had reviewed and/or tightened security policies. However, significant challenges remain; only 25% of respondents had performed a total risk assessment in the past six months.

“Given how fast things evolve in most of today’s environments, six months can be an eternity,” said Andy Norton, European Cyber Risk Officer at Armis. “This means that 75% of respondents are providing their boards with out-of-date and stale data that is not fit for timely risk assessments. Organisations can and should aim higher, particularly as capabilities now exist for performing continuous risk assessments, which can help them achieve the next crucial step towards risk assessment maturity.”

When it comes to the geopolitical landscape, three in five respondents said they’re dealing with more security alerts, and almost two-thirds expressed worries about Russian attacks on UK critical national infrastructure (CNI).

“Given the security environment in Europe, it is crucial that organisations in NATO countries continue to shore up defences and scale up the ability to handle a growing number of vulnerabilities. Insights revealed in this survey highlight that, yes, businesses are making some progress, but there is room for improvement when it comes to providing business leaders with real-time information that will help them allocate the right resources and make the best decisions regarding their cybersecurity strategies,” concluded Norton.

About Armis

Armis is the leading unified asset intelligence platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

Armis

Armis

pr@armis.com

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Other](#)

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.

© 1995-2022 Newsmatics Inc. All Right Reserved.