# Armis State of Cyberwarfare and Trends Report 2022-2023 Highlights Australia IT Professionals' Sentiment on Cyberwarfare

*Concerns about the threat of cyberwarfare are impacting business decisions in Australia*

MELBOURNE, AUSTRALIA, January 26, 2023 /EINPresswire.com/ -- Armis, the leading asset visibility and security company, today announced preliminary findings from the Armis State of Cyberwarfare and Trends Report: 2022-2023, which highlights global IT and security professionals' sentiment on cyberwarfare. The study shares responses from more than 6,000 respondents across multiple industries, including 511 professionals from Australia.

The Russian invasion of Ukraine has not only tragically upended the lives of countless people in a sovereign nation, but is also causing geopolitical shockwaves of cyberwarfare that will reverberate for the foreseeable future. Today's targets extend well beyond governments; any organization is a potential victim, with critical infrastructure and high-value entities at the top of the list.

"Cyberwarfare is the future of terrorism on steroids, providing a cost-effective and asymmetric method of attack, which requires constant vigilance and expenditure to defend against," said Nadir Izrael, CTO and Co-founder at Armis. "Clandestine cyberwarfare is rapidly becoming a thing of the past. We now see brazen cyberattacks by nation-states, often with the intent to gather intelligence, disrupt operations, or outright destroy data. Based on these trends, all organizations should consider themselves possible targets for cyberwarfare attacks and secure their assets accordingly."

"Many Australians have felt the effects of cyberwarfare first hand through the ongoing fallout from the Optus and Medibank breaches," said Evan Thomas, Partner Business Manager ANZ, Armis."Threat levels are increasing across the region and Australia is no exception, with resources that should be going into building businesses being diverted to tackle this situation instead.  In order to refocus on growth, firms need to take a strategic view of cyberwarfare and secure their assets accordingly."

Key findings from the Armis State of Cyberwarfare and Trends Report: 2022-2023 include:

- Forty percent of Australian respondents experienced more threat activity on their networks between May and October 2022 when compared to the six months prior, and over half (57%)

have experienced a cybersecurity breach at their organization.
- Australian firms are the most likely (79%) in the world to have stalled or stopped digital transformation projects due to the threat of cyberwarfare, above the global average of 55%.
- Sixty-six percent of respondents say they are reconsidering suppliers as a result of the Russia-Ukraine conflict - more than the average across the APJ countries we surveyed (54%) and also more than the global average (51%).
- Ninety-two percent of Australian respondents are confident in their government's ability to defend against cyberwarfare despite the string of recent, high-impact breaches.

For further information on the Armis State of Cyberwarfare and Trends Report: 2022-2023 visit: https://www.armis.com/cyberwarfare/

Methodology
Armis surveyed 6,021 IT and security professionals in firms with more than one hundred employees across the UK, USA, Spain, Portugal, France, Italy, Germany, Austria, Switzerland, Australia, Singapore, Japan, the Netherlands, and Denmark. Those findings were gathered between September 22, 2022 and October 5, 2022 and depict the state of cyberwarfare globally across various regions and industries including financial services, healthcare, critical infrastructure, retail, supply chain and logistics, and more. From the APJ region, Armis surveyed 511 individuals in Australia, 501 in Japan, and 501 in Singapore.

About Armis
Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 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 cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

Armis
Armis
email us here
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/613373662

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.