

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

Singapore firms amongst the top three most likely in the world to have stalled or stopped digital transformation projects due to the threat of cyberwarfare

SINGAPORE, 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 501 professionals from Singapore.

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."

"Singapore is known worldwide as a technology and innovation hub, but our survey suggests this status is under threat. Results confirm that cyberwarfare is stalling or even stopping digital transformation projects across the city state, and threat activity is on the rise," said Gwen Lee, Regional Director ASEAN, Armis. "To change this situation, organizations need to take a strategic view of cyberwarfare and secure their assets accordingly, allowing them to refocus on growing their businesses."

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

- Sixty-three percent of Singaporean respondents agreed that their firm had stalled or stopped

digital transformation projects due to the threat of cyberwarfare, putting the city-state amongst the 3 most likely in the world to have those projects affected.

- Three in five (60%) IT and security professionals surveyed in Singapore have experienced a cybersecurity breach at their company.
- Thirty-six percent of local respondents indicated they've experienced more threat activity on their networks between May and October 2022 when compared to the six months prior. Healthcare and telecommunications firms have seen the highest increase.
- A large majority of Singapore respondents (83%) believe their companies have allocated sufficient budget for cybersecurity programs, people, and processes.

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

[email us here](#)

Armis

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/613372510>

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.