Armis releases Armis State of Cyberwarfare and Trends Report: 2022-2023

Only one-third of UK organisations have a validated plan in place to handle cyberwarfare

LONDON, UK, January 24, 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 measures global IT and security professionals' perceptions of cyberwarfare. It found that while 84% of UK organisations claimed they had programmes and practices in place to respond to cyberwarfare threat, only one-third (32%) said their plans are validated by best practice frameworks, which is less than the global average of nearly 40%. In addition, 57% of UK organisations have stopped or stalled digital transformation projects due to threat of cyberwarfare - slightly higher than the global average of 55%.

The growing threat of cyberwarfare
The Russian invasion of Ukraine has not only tragically upended the lives of countless people in a sovereign nation, but it is also causing geopolitical shockwaves of cyberwarfare that will reverberate for the foreseeable future. Today's targets extend well beyond the higher levels of the opposition governments; any organisation is a potential victim, with critical infrastructure and high-value entities at the top of the list. The study shares responses from more than 6,000 respondents globally and across multiple industries, including healthcare, critical infrastructure, retail, supply chain and logistics, and more.

The study showed that cyberwarfare was one of the lowest-ranking priorities for UK organisations – despite a majority of organisations (59%) agreeing that the threat of cyberwarfare has increased since the start of the Ukrainian conflict, and 62% claiming to be somewhat or very concerned about the threat of cyberwarfare on their organisations. In the UK, for instance, 42% of security professionals claimed to have had to report an incident of cyberwarfare to authorities, which is significantly higher than the European average of one-third of companies, but lower than the global average of 45%. A further 28% of UK organisations reported more threat activity on their networks in the past six months compared with the six months prior.

Other interesting UK figures include:
- Almost half (46%) of UK security professionals have said they're reconsidering suppliers as a result of the Ukrainian conflict.
- Almost three-fifths (57%) of UK security professionals support a conscription to a cyber

defence league if the UK was drawn into a cyberwar conflict.

- Almost one in ten (9%) of UK companies spend less than 5% of IT budget on cybersecurity, while the majority (43%) spend between 5-10%.
- When it comes to paying for ransomware, almost a quarter (24%) of security professionals in the UK said they have an “always pay” policy, while a quarter (25%) have a “never pay” policy and 31% would only pay if customer data was at risk.
- The UK has a relatively high confidence in its government protecting from cyberwarfare threats (77%), compared with the European average of just 67% being confident in their governments.

Observations on Network & Information Systems (NIS) Regulations

A majority of organisations in the UK somewhat (46%) or strongly (25%) support the extension of NIS regulations to all businesses, while 27% remain indifferent to the legislation. Historically, NIS regulations applied to operators of essential services and relevant digital service providers, but have since seen updates in the NIS2 iteration that extend to “important” services as well. The study also examined UK security professionals’ adoption of NIS and found that only one-third (33%) strongly agree that they have mapped their cybersecurity programmes to NIS.

A further 78% of organisations somewhat (41%) or strongly (37%) agree that they review cybersecurity risks coming from immediate suppliers, with 34% strongly agreeing that they are able to address vulnerabilities in their supply chains. However, when broken down into industry sectors, OT sectors in the UK fell significantly below this baseline average of being able to confidently address supply chain vulnerabilities at 28%. Almost half (46%) of UK security professionals in all sectors have said they’re reconsidering suppliers as a direct result of the Ukrainian conflict.

“The first of the minimum set of requirements for NIS2 is to have adequate risk analysis. This alone is a major issue for many essential or important entities, because risk analysis is founded on an understanding of the critical assets that comprise the essential function, and for most organisations an up to date and accurate asset register is either non-existent, out of date or partial at best,” said Andy Norton, European Cyber Risk Officer at Armis. “To validate cyber security expenditure is not simply a house of cards, it will be vital for organisations to prove their risk analysis is adequate and appropriate and in line with NIS2 law. The study indicates that UK organisations are taking some action to comply with new regulations and validate cybersecurity programmes against best practice frameworks, but also that there is still significant room for improvement."

For further information on the Armis State of Cyberwarfare and Trends Report: 2022-2023, including the availability of the full report, 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 (1003), 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.

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.

for Armis
Smile on Fridays
armis@smileonfridays.com
Visit us on social media:
Twitter
LinkedIn
