ARMIS®

THE STATE OF
CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

UNITED KINGDOM

TABLE OF CONTENTS

INTRODUCTION ---- 03

SUMMARY OF FINDINGS ---- 04

EMEA ---- 05

Regulation is pushing towards the future ---- 06

UK TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023 ---- 07

The threat of cyberwarfare is hindering digital transformation for the majority of UK companies ---- 07

There is a disconnect between the mounting threat of cyberwarfare and the preparedness of UK organisations ---- 08

UK organisations are making plans, but failing to validate them with best practices ---- 08

Network & Information Systems (NIS) Regulations gain importance ---- 09

WHY DO THESE FINDINGS MATTER? ---- 11

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF? ---- 12

INTRODUCTION

If you've reviewed the global Armis State of Cyberwarfare and Trends Report: 2022-2023, you know that it's critical for business and IT leaders to understand the evolving threat landscape surrounding cyberwarfare, so that they can improve their cybersecurity posture to defend against these attacks. To prepare this report, Armis commissioned a study surveying 6,021 IT and security professionals globally to determine worldwide trends as they relate to security professionals' sentiments on cyberwarfare, attack patterns, cyber spending, and more. Responses were gathered between September 22, 2022 and October 5, 2022.

Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Proprietary data from the Armis platform collected June 1, 2022 through November 30, 2022 confirmed that cyberattacks haven't slowed, only worsened. Threat activity against the global Armis customer base increased by 15% from September to November when compared to the three months prior. Further, Armis identified the largest percentage of threat activity against critical infrastructure organizations, with healthcare organizations the second most targeted when compared to various industries.

In addition to these global findings, Armis has prepared regional findings and country-by-country analysis to offer unique, localized insights which may be more impactful for individual readers depending on where they physically are based and the counties in which their business operates. **For this country-by-country analysis, we will zoom in on the findings pulled from the 1,003 respondents who shared insights for our survey that are based out of the United Kingdom and work across industries including healthcare, manufacturing, retail, and more.**

SUMMARY OF FINDINGS

Overall, Armis identified four key trends when analysing responses from IT and security professionals from British companies when compared to other global respondents from EMEA, the U.S., and APJ. Below, we dive deeper into those findings and the trends they're indicative of.

It found that a majority of UK organisations have had to stop or stall digital transformation projects, with databases and PII deemed most at risk in the event of a cyberwarfare attack. And while the threat of cyberwarfare comes low on the priority list for security professionals, the majority acknowledge that the conflict in Ukraine has increased the concern of cyberwarfare on their businesses and services they provide.

Furthermore, with mounting regulatory obligations for UK organisations, the adoption of Cyber Risk Frameworks and mapping cybersecurity programmes to best practices remains relatively low compared with the rest of the world.

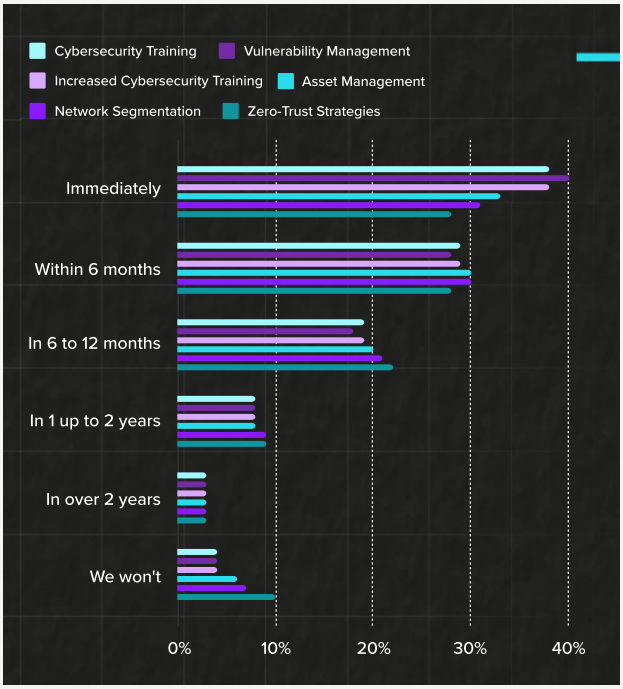
EMEA

Through the course of 2022, the EMEA region has been shocked by the invasion of the sovereign nation of Ukraine. With the geopolitical instability associated with physical warfare and cyberwarfare, shockwaves of consequences are arriving throughout the area. Unpredictability in the food supply, the infamous energy crisis, and a wave of cyberattacks focused against the most critical functions of society, are all contributing to changes in spending and priorities across numerous industries. The report confirms the rise in cyberattacks, bringing to light that almost 3 in 5 organisations (58%) experienced one or more cybersecurity breaches. And 25% of respondents confirmed that there has been an escalation in the number of threats to their organisation.

Measures are being taken to ensure protection, but to date, still less than half (44%) of IT and security professionals agree that their organisation has programs and practices in place to respond to cyberwarfare threats. Respondents depicted their company as ill-prepared as there are some relevant issues to be addressed:

- Only 46% of IT and security professionals in EMEA strongly agreed on knowing who to contact if they notice suspicious activity.
- Only 76% of IT and security professionals in EMEA said they collaborate with others in the industry when it comes to sharing information about threats, below the U.S. and APJ averages. Although being a high number, this indicates that there is still work to be done if all areas are to be shielded from cyberattacks.
- Only 33% of IT and security professionals in EMEA have reported an act of cyberwarfare to the authorities, below the US (63%) and APJ (61%) levels.
- Almost 2 in 10 (18%) of IT and security professionals in EMEA said their organisation does not have a contingency plan in place if cyberwarfare is detected.
- Only a third (33%) of IT and security professionals have a validated cyberwarfare plan with best practice frameworks, to be appropriate and proportionate.
- Moreover, less than half (49%) of companies are educating employees as a common practice, or restricting network admin rights (40%). Fewer still have cybersecurity practices implemented such as creating a security-focused work culture (37%), investing in cybersecurity insurance (31%), and implementing a Cyber Risk Framework (31%).

There is a disconnect between confidence levels of preparedness for cybersecurity attacks (84%) and reality, and investment is needed to close that gap, both for tools and services. When asked to select when they will invest in certain aspects, the following responses were given by IT professionals:



REGULATION IS PUSHING TOWARDS THE FUTURE

Governments, security services and related competent authorities continue to put great emphasis on the need for an improved cybersecurity posture, and the imperative necessity for a more cyber resilient strategy. The recent EU Cyber Resilience Act builds on the EU's existing Cybersecurity Directive of 2016, thus updating the bloc's requirements for enhanced cybersecurity by member states. Prior to this EU Cyber Resilience Act, much of the pressure when it came to cybersecurity was put on users of these products, both enterprises and individuals alike. Now, the manufacturer will share a larger part of this responsibility as well. Accountability can go a long way in helping to make improvements across the board. The EU also released NIS2, adding many more verticals into the spotlight and introducing fines, sanctions, and penalties, for not doing proper risk management, basic cyber hygiene, and taking undue delays in corrective action.

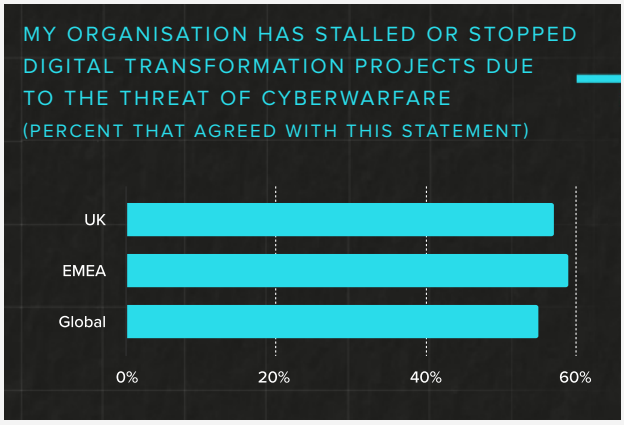
The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected assets. 37% of respondents agree that connected devices are a top priority in the event of a cyberwarfare attack.

Beyond the internal efforts, it is believed amongst IT professionals that the European Union and its member states should also boost cooperation with other allies around the world. More than half (61%) stated that they would support conscription into a cyber defence league if their country were drawn into a cyberwar conflict.

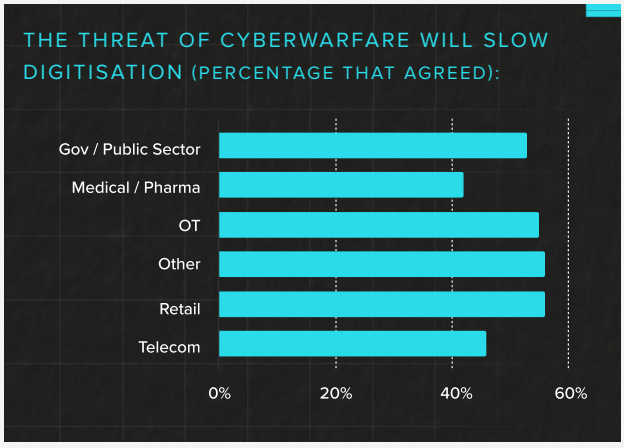
UK TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

THE THREAT OF CYBERWARFARE IS HINDERING DIGITAL TRANSFORMATION FOR THE MAJORITY OF UK COMPANIES

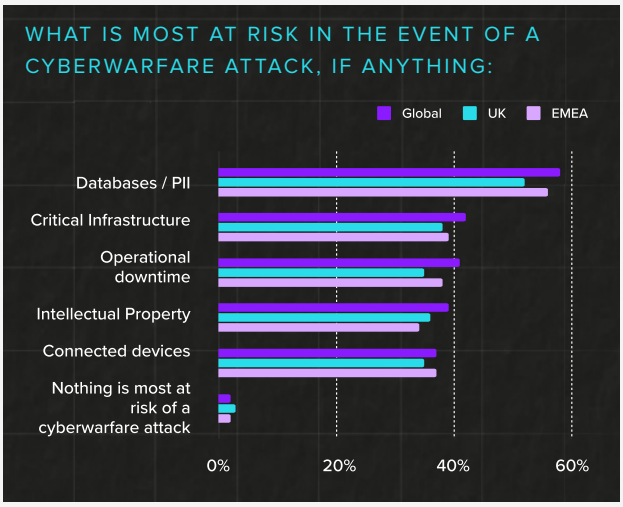
An alarming 57% of UK organisations say they have stopped or stalled digital transformation projects due to the threat of cyberwarfare - slightly higher than the global average of 55%.



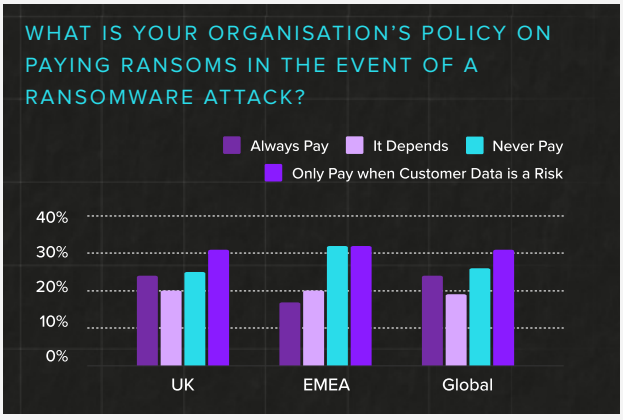
A further 53% said the threat of cyberwarfare will slow digitisation altogether. Interestingly, the majority (56%) of the Retail and Wholesale industry and 55% of OT organisations thought the threat of cyberwarfare would slow digitisation, while only 42% of Medical, Healthcare, Pharmaceutical organisations indicated the same.



In addition, 61% of UK organisations are somewhat or very concerned about the impact of cyberwarfare on their companies' services and called out databases and Personally Identifiable Information (PII) as the top risks in the event of a cyberwarfare attack.

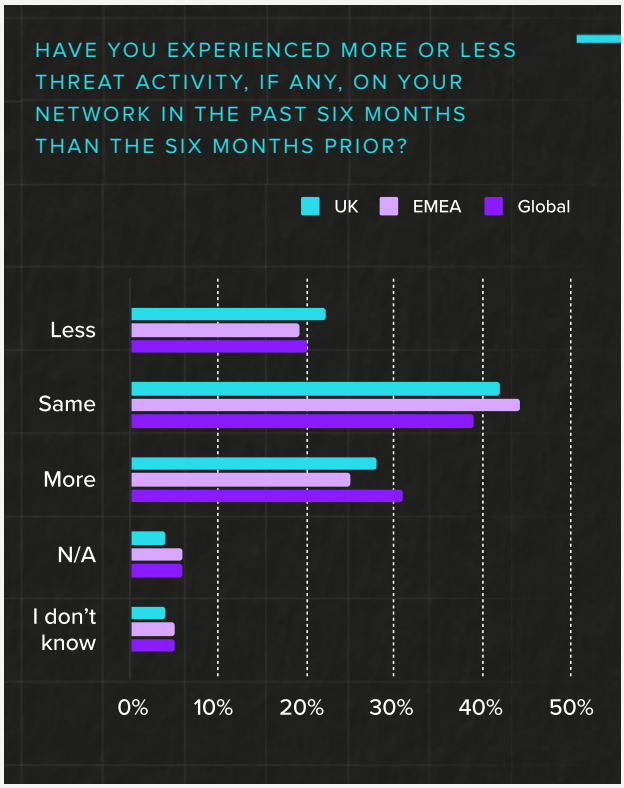


When it comes to paying for ransomware, 31% of UK organisations would only pay if customer data was at risk. Almost a quarter (24%) of security professionals in the UK said they have an "always pay" policy, while a quarter (25%) have a "never pay" policy.

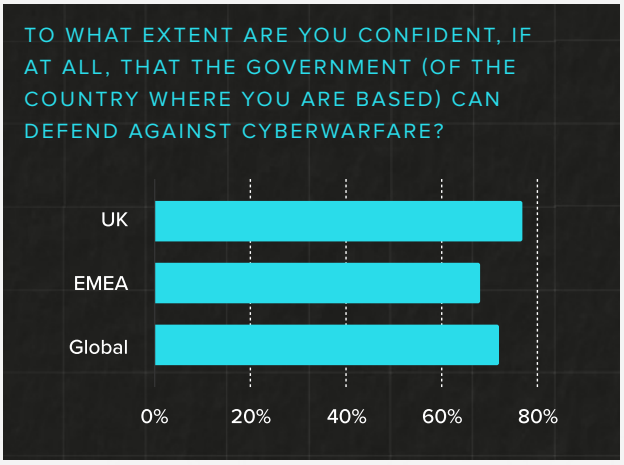


THERE IS A DISCONNECT BETWEEN THE MOUNTING THREAT OF CYBERWARFARE AND THE PREPAREDNESS OF UK ORGANISATIONS

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.

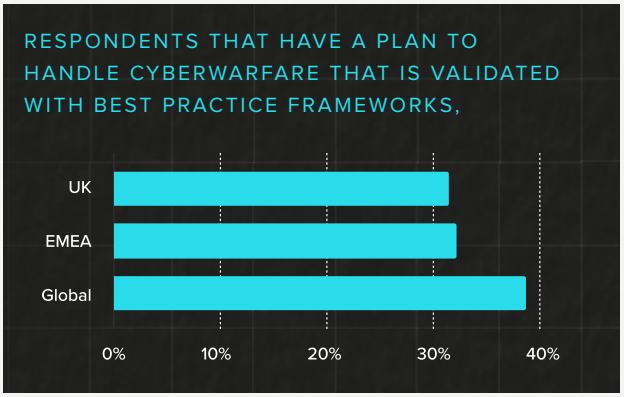


Though, somewhat encouragingly, The UK has a relatively high confidence in its government protecting from cyberwarfare threats (77%), compared with the European average of just 67% being confident in their governments. Furthermore, almost three-fifths (57%) of UK IT and security professionals support conscription into a cyber defence league if the UK was drawn into a cyberwar conflict.

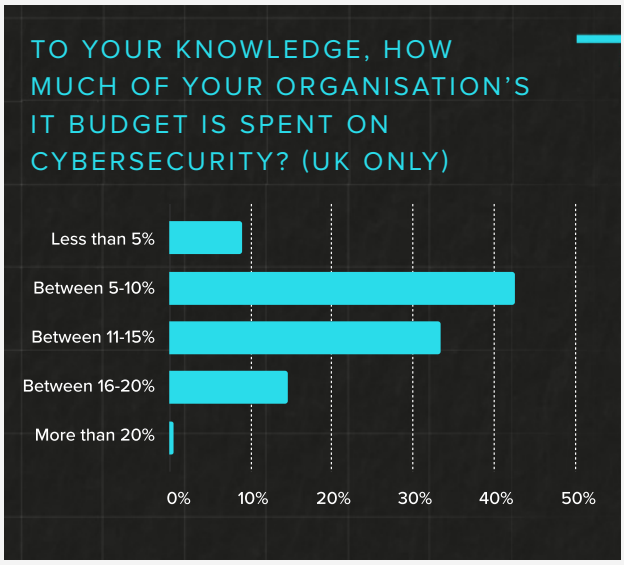


UK ORGANISATIONS ARE MAKING PLANS, BUT FAILING TO VALIDATE THEM WITH BEST PRACTICES

The study found that while the majority 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%.



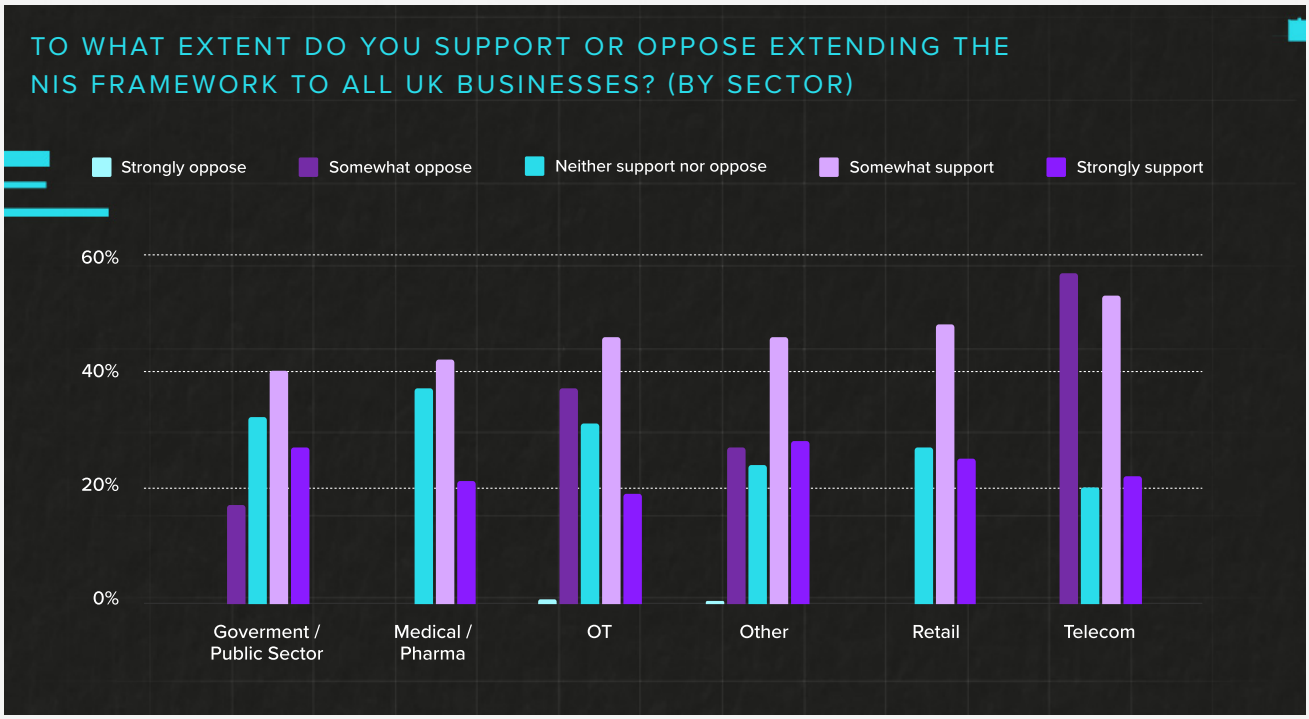
In terms of cybersecurity spend, Almost one in ten (9%) of UK companies spend less than 5% of IT budget on cybersecurity, while the majority (43%) spend between 5-10%.



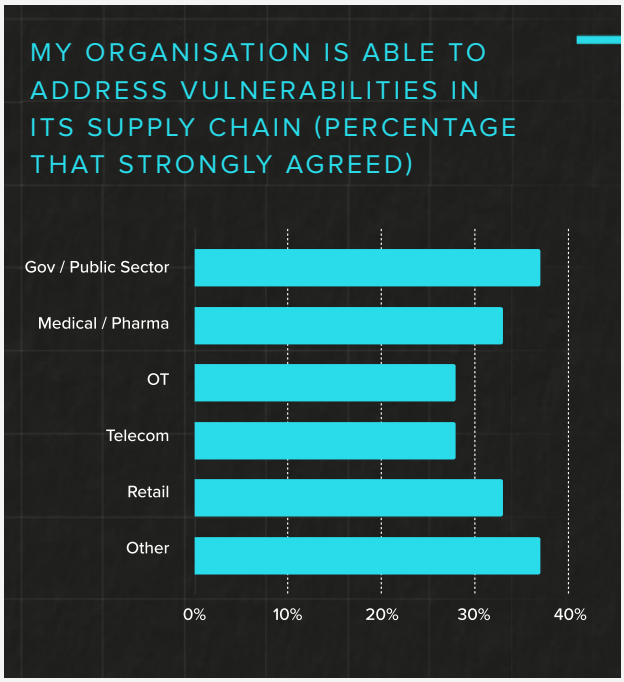
NETWORK & INFORMATION SYSTEMS (NIS) REGULATIONS GAIN IMPORTANCE

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.



WHY DO THESE FINDINGS MATTER?

The findings are a significant indication of the current landscape against a backdrop of the recently launched 2022 CyberSecurity Incentives and Regulation Review in the UK to further refine its legislative measures for enhanced cyber resilience with regard to changes in cyberwarfare and recent technological developments. This builds upon the existing Network and Information Systems Regulations 2018 (NIS Regulations), of which newer iterations (NIS2) will give organisations that provide important services to the public 21 months to comply or risk fines. In addition, further strengthening of cybersecurity related to connected assets is expected in the UK if the amended Product Security and Telecommunications Infrastructure Bill passes.

> *"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," ... "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."*
>
> **ANDY NORTON**
> EUROPEAN CYBER RISK OFFICER AT ARMIS

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF?

So, what can organizations do? Early detection and continuous monitoring is the best way to improve your organization's security posture and remediate quickly. After all, if you don't know you have a problem, you can't fix it. Similarly, if you can't see an asset, you can't protect it. This is where Armis can assist.

ARMIS ASSET INTELLIGENCE PLATFORM

The **Armis Asset Intelligence Platform** provides unified asset visibility and security across all asset types, including information technology (IT), internet of things (IoT), operational technology (OT), internet of medical things (IoMT), cloud, and cellular-IoT — both managed and unmanaged. Delivered as an agentless software-as-a-service (SaaS) platform, Armis seamlessly integrates with existing IT and security stacks to quickly deliver the contextual intelligence needed for improving an organization's security posture, without disrupting current operations or workflows. Armis helps customers protect against unseen operational and cyber risks, increase efficiencies, optimize the use of resources, and safely innovate with new technologies to grow their business – no matter the threat, cyberwarfare or other.

Register today for a Security Risk Assessment to learn which assets are most vulnerable to attack. Use these insights to prioritize your risk mitigation strategy and ensure full compliance with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

To request a custom demo from Armis, please visit: armis.com/demo.

To dive deeper into the findings of the Armis State of Cyberwarfare and Trends Report: 2022-2023 on a global scale, please visit: **armis.com/cyberwarfare.**

THE STATE OF
CYBERWARFARE

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.com

info@armis.com

20230110-1

ARMIS®