ARMIS®

THE STATE OF
CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

DENMARK

TABLE OF CONTENTS

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 50 respondents who shared insights for our survey that are based out of Denmark and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

Overall, Armis identified six key trends when analyzing responses from IT and security professionals from Danish 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.

The UN recently ranked Denmark as the world leader in digital infrastructure according to the E-Government Survey 2022, emphasizing that Denmark is a highly digitalized country. Danish companies have been focusing on digitizing production and industry operations, bringing more connected devices into the IT environments. However, many companies – especially in the country's large production industry – are still using legacy systems in some parts of their operations that are not designed with cybersecurity in mind. This can create an opening for hackers to exploit the systems and gain access to the network. Due to Denmark's high level of digitalization, hackers find large Danish companies and state-owned businesses attractive. In the past five years, we have seen successful attacks on Mærsk, Vestas Wind Systems, William Demant, and the National Danish Railways DSB.

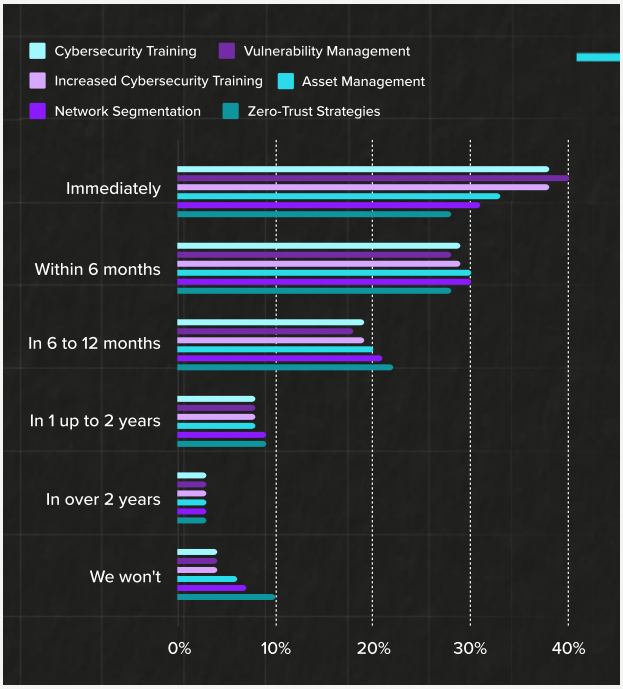
EMEA

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.

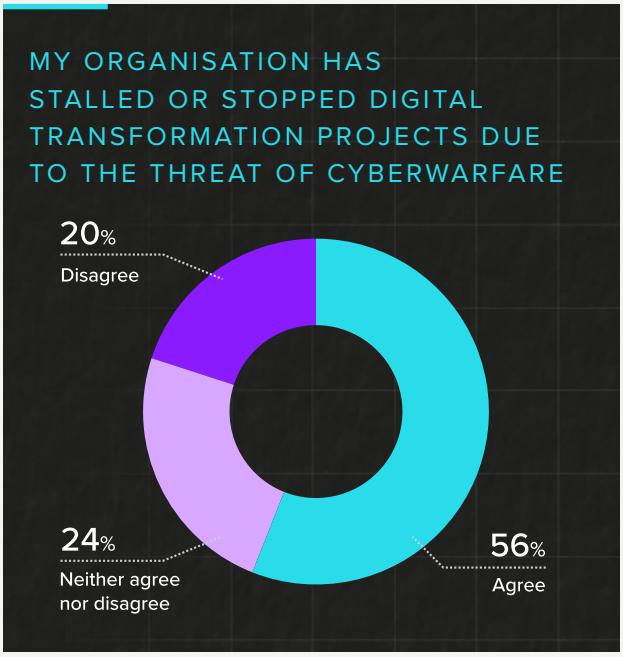
The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected 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.

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

DANISH COMPANIES ARE STALLING DIGITAL TRANSFORMATION DUE TO CYBERWARFARE THREATS

More than 4 in 5 (84%) respondents agree that both the public and private sector should be involved in defining public policies around cybersecurity, similar to what happened in the Grenelle for ecology in 2007. Even though high percentages seem to agree that there will be increased regulation and that companies should be involved in public policies, only 53% have implemented backing up data as a cybersecurity practice in their organisations. Even fewer are using anti-malware and firewall software (48%), encrypting data (46%), or implementing a Cyber Risk Framework (41%). This might suggest they will be somewhat unprepared for stricter regulations.



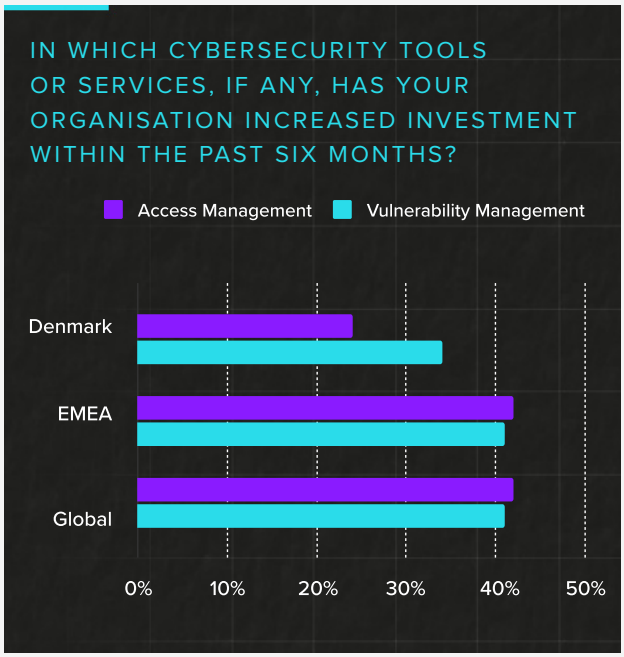
THERE'S NO INDICATION OF HACKERS SLOWING DOWN

74% of all Danish companies in the research have experienced the same or a higher level of threat activity towards their systems in the most recent six months compared to the six months prior. 34% of this 74% answered that they have experienced higher threat activity, indicating that hackers are not planning on slowing down on attacking Danish companies. These results are above the EMEA average where 25% have experienced a higher level of threat activity in the same period. A potential explanation for Danish companies being targeted lies in the fact that Denmark is one of the most digitized countries in the world.

> *"The results may be surprising for many, but this correlates perfectly with what I hear from our Danish customers. There are very few companies experiencing a decrease in threats towards their network. A part of the explanation might be that we have been filling our production lines and other areas of the business that needed to be modernised with thousands of unsecured connected devices which hackers are happy to use as attack vectors as they are difficult to identify,"*
>
> **LARS HERMIND**
> REGIONAL SALES DIRECTOR, NORDICS AND BENELUX AT ARMIS

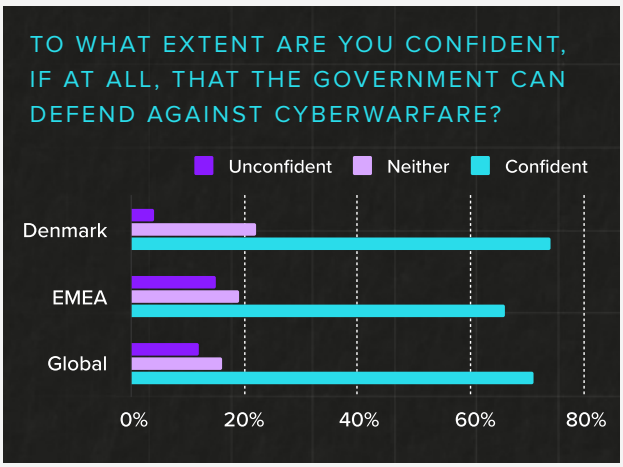
ACCESS MANAGEMENT IS NOT A PRIORITY FOR DANISH IT AND SECURITY PROFESSIONALS

When asked which cybersecurity tools or services companies have increased their investments within the past six months, Danish companies are somewhat behind in most categories with Vulnerability Management and Access Management being the most noticeable. Only 24% of the Danish companies have increased investments in Access Management compared to 42% in EMEA, while 34% have increased investments in Vulnerability Management in Denmark compared to an average of 41% in EMEA.



DANES TRUST IN THE GOVERNMENT'S ABILITIES TO DEFEND AGAINST CYBERWARFARE

The report also shows that Danish companies are more confident that the government can and will defend them against cyberwarfare, with 74% answering that they trust the government's abilities compared to an EMEA average of 66%. In Denmark, we have seen an increased political interest in securing Denmark's digital infrastructure against state-sponsored threat actors and hacker groups. Recently, the National Centre for Cyber Security also raised the threat level on different types of cyberthreats. The threat level for cyber espionage and cybercrime was categorised as being very high. The political focus on handling national cyber threats could be one of the reasons for companies' confidence in the government's abilities.



DANISH COMPANIES ARE MORE WILLING TO PAY HACKERS WHEN VICTIMS OF RANSOMWARE ATTACKS

Danish companies are more likely to pay ransom to hackers in the event of a ransomware attack, with 36% answering that they will always pay ransom compared to an EMEA average of 17%. 24% of Danish companies will never pay ransom compared to the EMEA average of 31%, while 26% will pay only if customer data is at risk. The average for EMEA is 32% if customer data is at risk. As Danish companies are more likely to pay a ransom, hackers might focus more on the region to maximise the possibility of getting paid.

MANY ATTACKS MAY LEAD TO A CYBER DEFENCE LEAGUE

More than one-third of the Danish companies in the report have had to report a cyberwarfare incident to the authorities. In the past years, we have seen a spike in direct and indirect cyberattacks in Denmark across all business sectors resulting in economic and operational damages. Perhaps that is part of the reason why 62% support the idea of a cyber defence league in the case of cyberwarfare. This is interesting considering the recent vote on whether Denmark should lift the opt-out on defence and thereby be able to join a future EU army or not. The opt-out was lifted and might have increased focus on transnational collaborations regarding defence.

WHY DO THESE FINDINGS MATTER?

The findings from the cyberwarfare report show that cyberattacks are influencing many business areas and that companies are prioritising very differently in their cybersecurity efforts regionally – some more or less surprising.

> *"In general, Danish companies are aware of the cyberwarfare threats. However, I often meet companies lacking a detailed cybersecurity strategy or a total overview of all their devices. This is of course a security concern – especially if companies don't know all their vulnerabilities. In that case, hackers could operate in the dark for months without the company ever knowing that their data is being compromised."*
>
> **LARS HERMIND**
> REGIONAL SALES DIRECTOR, NORDICS AND BENELUX 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®