THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

FRANCE

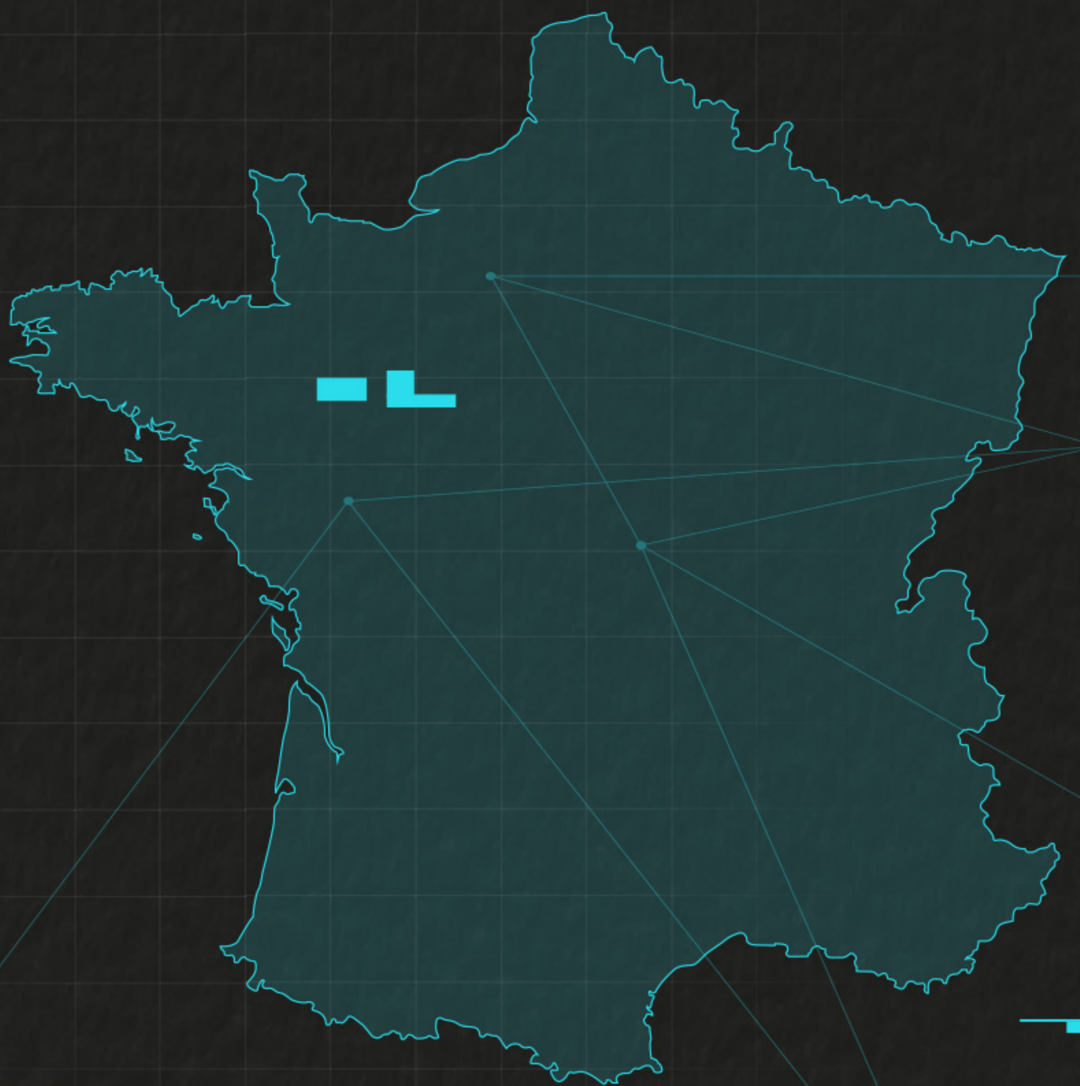


TABLE OF CONTENTS

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

SUMMARY OF FINDINGS

Overall, Armis identified four key trends when analyzing responses from IT and security professionals from French 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 global geopolitical context and the recent health crisis have often shown the lack of preparedness of some governments of industrialized countries in managing cybersecurity issues. Several organizations, insufficiently prepared or unaware of the flaws in their IT infrastructures, have been victims of extortion attempts that can take several forms. No sector has been spared by these attacks, starting with the so-called critical activities or those vital to the smooth running of companies. France has not been spared in recent years and continues to suffer from repeated attacks affecting both public and private organizations. Overall, there is a crisis of confidence in the ability of the authorities to protect assets. Armis asked IT and security professionals to answer the question of how much they trust the government, with 8% of respondents saying they have no confidence in the authorities' ability to protect assets. On the other hand, 16% say they have full confidence in the government. With stricter cybersecurity regulations coming to the EU, it is clear that trust in the government covers a wide range of opinions. The report also finds that organizations in France might not be fully prepared to embrace the incoming regulations.

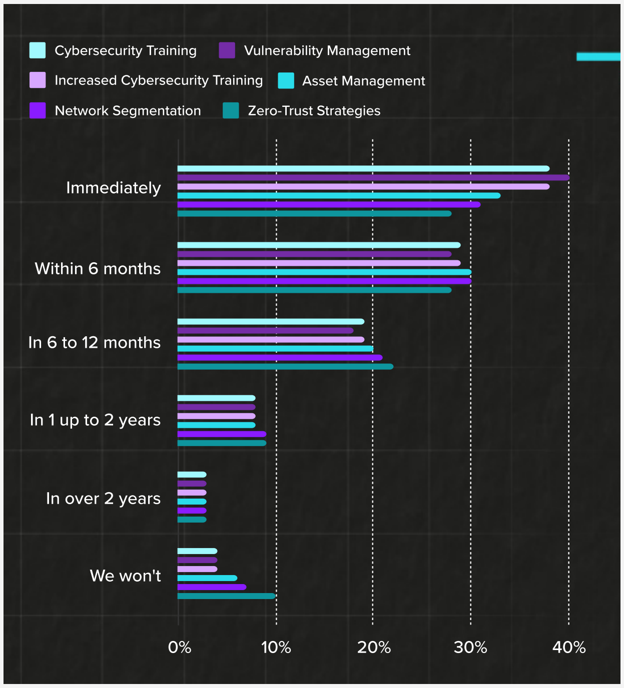
EMEA

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.

CYBERSECURITY: CRISIS OF CONFIDENCE OF FRENCH ORGANIZATIONS TOWARDS THE GOVERNMENT

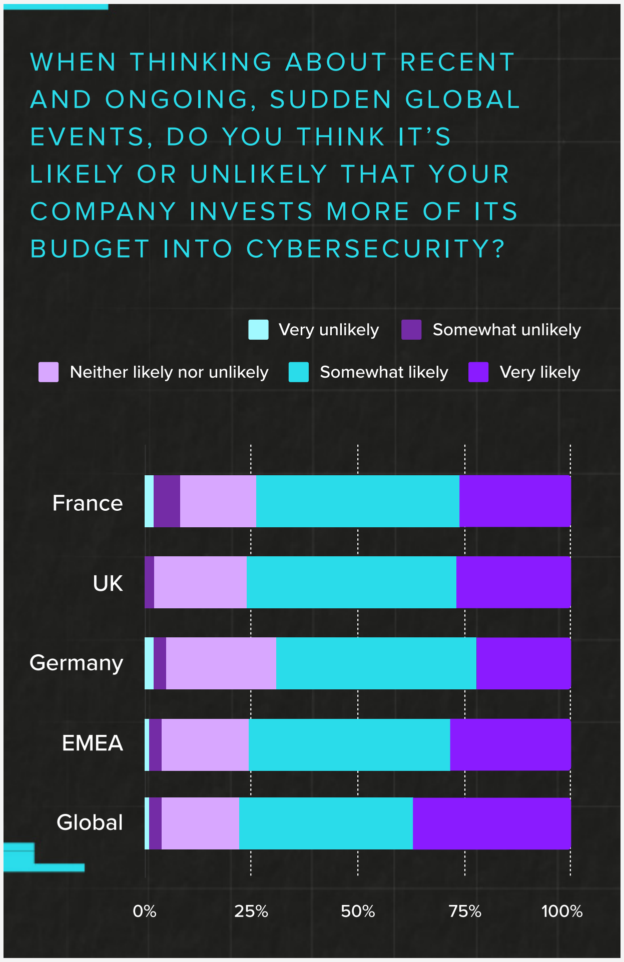
IMPENDING REGULATIONS VERSUS PREPAREDNESS

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.

ARE THE COMPANIES' CONCERNS IN VIEW OF THE GEOPOLITICAL CONTEXT CORRECT?

Recent events may have led some to believe that context-sensitive organizations would have increased their efforts and investment in cybersecurity. It is true that when thinking about recent and ongoing global events, 74% of companies will increase investment in cybersecurity, but 18% of French respondents would not be able to say whether more budget will be allocated to that function, and almost 2% consider it very unlikely that their organization will do so. These differ from other geographies such as the United Kingdom, where 22% have no idea. In Germany, 26% are not able to say, and 2% have serious doubts.

Surprisingly, some organizations are not considering social and economic indicators when deciding their budgetary orientations.



THE MEDICAL SECTOR UNDER PRESSURE, BUT LITTLE AFFECTED BY THE ATTACKS

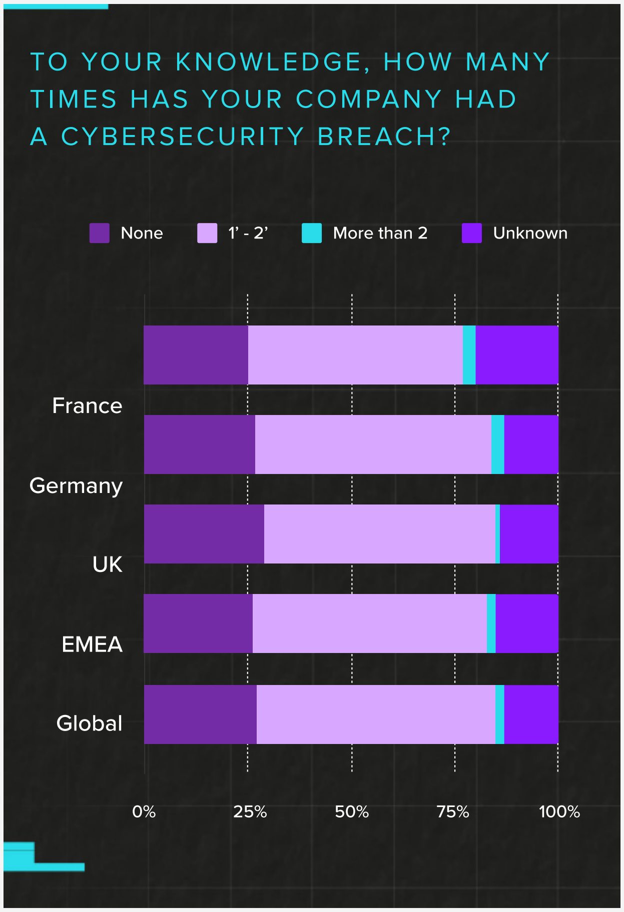
When we look at the healthcare sector in France, which has been the victim of repeated attacks during and after the pandemic, we find that despite a particularly difficult context and the consequences on the continuity of care, the sector seems little concerned. 22% are simply unconcerned about this phenomenon, while 9% do not feel at all concerned. On the other hand, 45% say they are relatively concerned while 13% are very concerned. At this stage, we understand that the attacks are not yet perceived as a factor that can directly influence the respondents. Should we attribute this lack of interest to the repeated nature of the attacks, which has made them a habit that no longer deserves attention?

This very French attitude of "I don't feel concerned" is not found in other countries, or to a lesser extent. In Germany, for example, 53% of respondents said they were concerned and 0% said they were not at all concerned. Only 11% of the respondents are not concerned at all about this threat. On the other side of the Channel, the approach is also different: in the UK 17% are simply unconcerned, 3% do not feel concerned at all and 49% are worried.

WHAT LESSONS CAN BE LEARNED FROM THE OPACITY OR COMMUNICATION OF ORGANIZATIONS IN REGARD TO CYBERATTACKS?

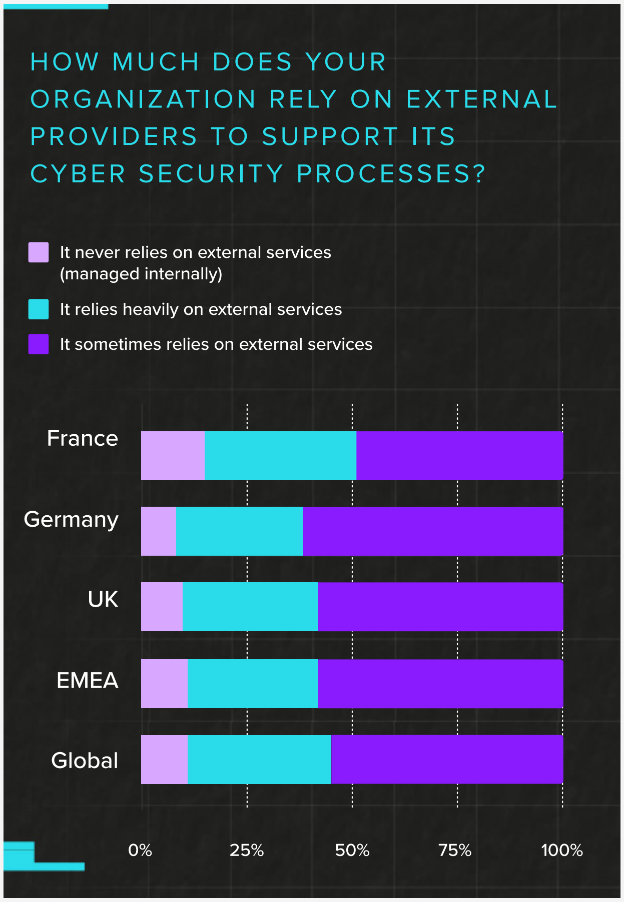
Organizations need to have both a reactive and proactive strategy for cybersecurity. And, if the number of attacks does not diminish, there's a question posed on what lessons to learn and how to help the ecosystem when its organization has been the victim.

In order to preserve their brand image and minimize the impact on their business, many organizations do not communicate about attacks. Yet this is valuable information that can be useful in understanding the processes used by cyber attackers. If attacks are not communicated appropriately, consequences can be worsened. Despite that, 20% of French respondents say they don't know if their organization has been affected by a cyberattack. And just half 52% say they have been informed that the company has been hit 1 or 2 times by an attack. Compared to their German neighbor, for example, only 13% say they have no information at all, against 57% who say they have been informed of an attack 1 to 2 times. On the British side, 13% have no knowledge of attacks that could have been carried out, and 56% are informed that an attack has been carried out 1 to 2 times. What can we learn from this? Perhaps organizations are more affected than we think and there is also work to be done in this area.



IN-HOUSE OR CONTRACTOR RESOURCES - WHO TO RELY ON?

How much of a role do IT providers play in implementing security protocols? It's true that organizations are bearing the brunt of repeated attacks. 15% of respondents report that their organization has never used a cybersecurity provider, but instead relies on in-house talent. 49% use a service provider from time to time. Here too, it must be understood that they have carried out a diagnosis to assess existing vulnerabilities or that they have been the victim of an attack and are not able to respond internally.In Germany, 8% say they do not rely on the skills of an external IT service provider, while 61% say they rely on the skills of a service provider outside the organization. In the UK, nearly 10% said they do not use the skills of a service provider, while 58% said they sometimes use them.



WHY DO THESE FINDINGS MATTER?

What we understand is that the road ahead in the fight against cyberattacks promises to be long. We observe that despite the unstable geopolitical context, companies do not seem to learn from macroeconomic events. On the employees' side, either some are not informed of the state of the attacks targeting their organization, or their employer resorts to service providers to respond to the lack of internal resources. The fight against cyber-attacks therefore requires a general awareness and of course a massive investment in employee training or the use of partners with the necessary expertise.

> *"Today, we have enough hindsight to say that while the recent health crisis has accelerated cyberattacks against private and public organizations, it has also shown that IT infrastructures are aging and inadequate against the new threats. Here, our study reveals that we have sadly failed to learn from the past; as management continues to fail to make asset protection a priority: the increase of budgets dedicated to the redesign of infrastructures is not at the center of discussions, the use of expert cybersecurity providers remains low and is still limited to audits that are only valid at the moment and not continuous, and the geopolitical and economic context does not seem to be a strong influence in the decision-making of companies. Without wishing to paint too bleak a picture of the state of cybersecurity in the EMEA region, we are faced with a form of cybersecurity paralysis, reinforced by successive crises, which is damaging performance."*
>
> **JEAN-MICHEL TAVERNIER**
> DIRECTOR FRANCE 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®