ARMIS®

THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

IBERIA

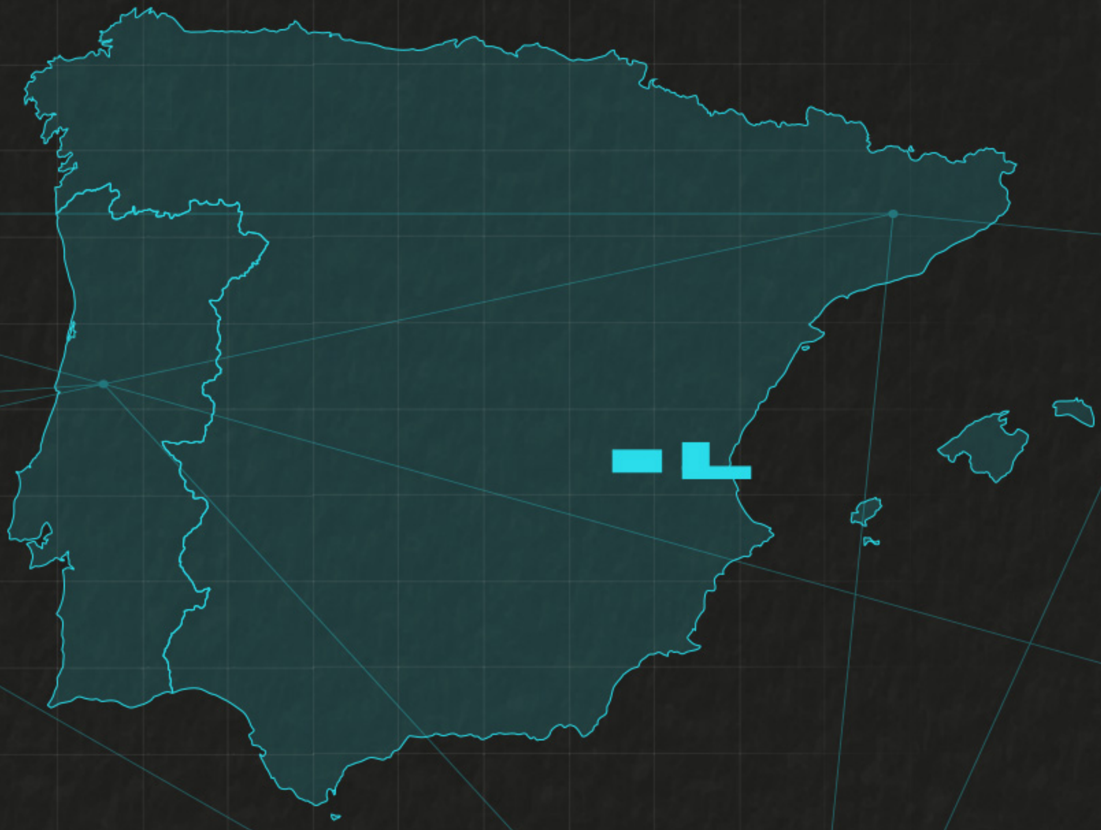


TABLE OF CONTENTS

INTRODUCTION ---------- 03

SUMMARY OF FINDINGS ---------- 04

EMEA ---------- 05

Regulation is pushing towards the future ---------- 06

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

Spanish organizations are the most worried in Europe about cyberwarfare ---------- 07

The threat landscape has stalled or stopped digital transformation projects in Spain ---------- 07

Lack of digital sovereignty and investment in the Spanish compendium of legislation and laws applied to cybersecurity ---------- 08

Cybersecurity spending continues to increase as boards change their organization’s culture towards it ---------- 08

Sectors at risk but ready to respond ---------- 09

PORTUGAL TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023 ---------- 10

Cyberwar worries Portuguese companies, which feel unprepared to deal with the event ---------- 10

Only a fraction of Portuguese companies are holding back on their digital transformation projects ---------- 10

Data protection is a top priority among Portuguese professionals ---------- 11

Portuguese companies are investing in the training of their employees regarding online security, but there are still efforts to be made in this area ---------- 12

Most Portuguese companies should invest more of their budget in cybersecurity ---------- 12

Portuguese trust the government’s ability to defend itself from a cyberfarware ---------- 12

WHY DO THESE FINDINGS MATTER? ---------- 14

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF? ---------- 15

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 751 respondents who shared insights for our survey that are based out of Spain (500) and Portugal (251) and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

According to the Armis study, Spain is the European country most worried about the threat of cyberwarfare. Nearly three in four (74%) Spanish organizations are concerned about the challenges that these global events might pose to the country, a figure higher than the global average (67%), and above Portugal (62%) which is closer to the European (60%) average. Due to the conflict in Europe, there has been an increase in cyberattacks in the region, which was clearly displayed in recent attacks on the public administration in Spain, as well as Portuguese and Spanish healthcare institutions.

> *"Recent cyberattack events show that attacker behavior is constantly evolving and that they have found alternative ways to evade traditional detection and response systems. We are in a complex environment, where there is no defined security perimeter to protect our assets. This is why it is relevant to understand the state and trends of cybersecurity in our companies."*
>
> **VESKU TURTIA**
> REGIONAL DIRECTOR, IBERIA, ARMIS.

Overall, Armis identified five key trends when analyzing responses from IT and security professionals from Iberian companies when compared to other regions. Below, we dive deeper into those findings and the trends they're indicative of.

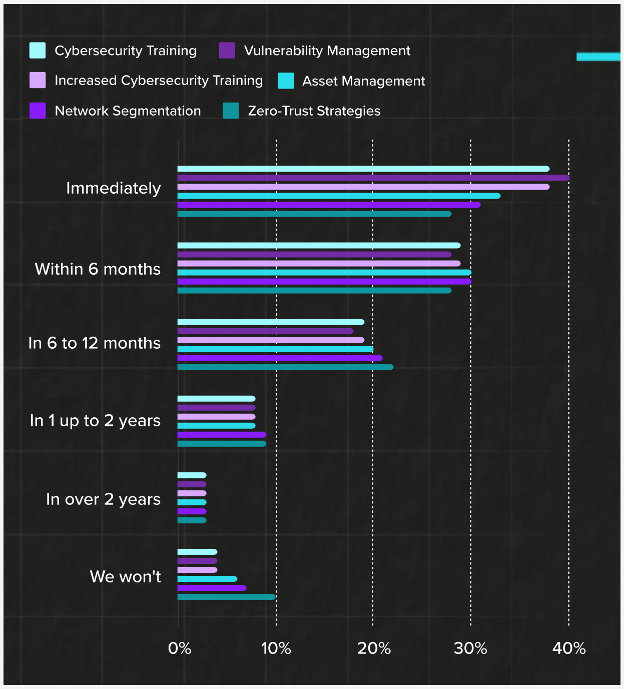
EMEA

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.

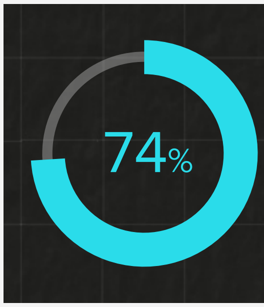
The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected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

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

SPANISH ORGANIZATIONS ARE THE MOST WORRIED IN EUROPE ABOUT CYBERWARFARE

74% of Spanish organizations are concerned about the threat of cyberwarfare, a number well above most regions and their counterparts in Europe. Despite the concern, more than a quarter of Spanish organizations (26%) feel unprepared to deal with cyberwarfare, and prevention against nation-state attacks is the least valued security element among IT professionals - not only in Spain but worldwide (22%). Data protection (67%) and intrusion detection (58%) remain the top priorities in region.



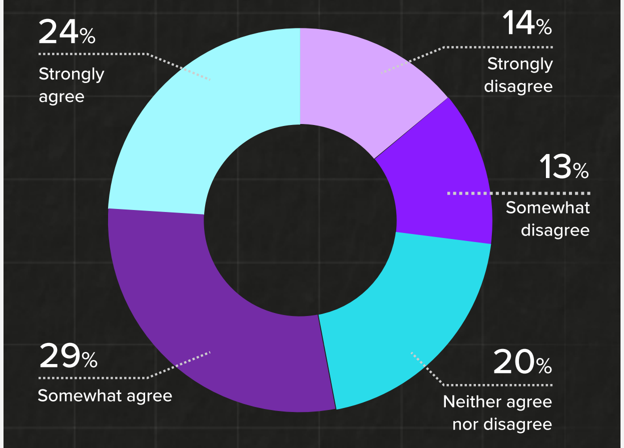
OF SPANISH ORGANIZATIONS ARE CONCERNED ABOUT THE THREAT OF CYBERWARFARE

Growing geopolitical tensions resulting from the war in Ukraine have made the threat of cyberwarfare attacks far more plausible. More than 67% of Spanish IT and security professionals surveyed by Armis agree that the war in Ukraine has created a greater threat of cyberwarfare, with 39% of respondents who are the sole decision-maker for IT security saying they experienced more threat activity on their network between May and October 2022 when compared to the six months prior, a rather low figure when compared with the global one (54%) but aligned with the European average (40%).

THE THREAT LANDSCAPE HAS STALLED OR STOPPED DIGITAL TRANSFORMATION PROJECTS IN SPAIN

The worsening threat landscape mentioned above has tangibly impacted digitization projects, possibly slowing innovation worldwide. Over half (53%) of Spanish IT professionals surveyed say that their organizations have stalled or stopped digital transformation projects due to these threats.

MY ORGANIZATION HAS STALLED OR STOPPED DIGITAL TRANSFORMATION PROJECTS DUE TO THE THREAT OF CYBER WARFARE

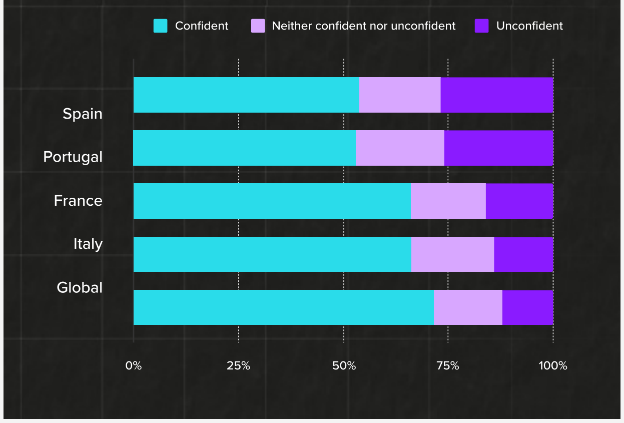


And 58% of Spanish respondents agree that the threat of cyberwarfare can be a stopper on digitalization for the country, a figure even higher than the European average (51%).

LACK OF DIGITAL SOVEREIGNTY AND INVESTMENT IN THE SPANISH COMPENDIUM OF LEGISLATION AND LAWS APPLIED TO CYBERSECURITY

Digital sovereignty is a relatively recent concept, described by the World Economic Forum as “the ability to have control over one’s digital destiny,” including “the data, hardware, and software” that someone “creates” and that someone “trusts.” Anxiety over the control and privacy of this data by European governments was a major factor in the introduction of the General Data Protection Regulation (GDPR). When referring to the cybersecurity legislation in Spain, 83% of Spanish respondents agree that there is a lack of digital sovereignty and investment. Historically, Spain has always lacked strong R&D investment. Spain ranks 17th in Europe, with a spend of 1.4% of its GDP on R&D while Europe’s average is 2.3%. Nevertheless, more than half (52%) of Spanish respondents say they are confident in the government’s ability to defend itself against cyberwarfare, a figure similar to Portugal but lower than in France or Italy (66% in both cases).

TO WHAT EXTENT ARE YOU CONFIDENT, IF AT ALL, THAT THE GOVERNMENT (OF THE COUNTRY WHERE YOU ARE BASED) CAN DEFEND AGAINST CYBERWARFARE?

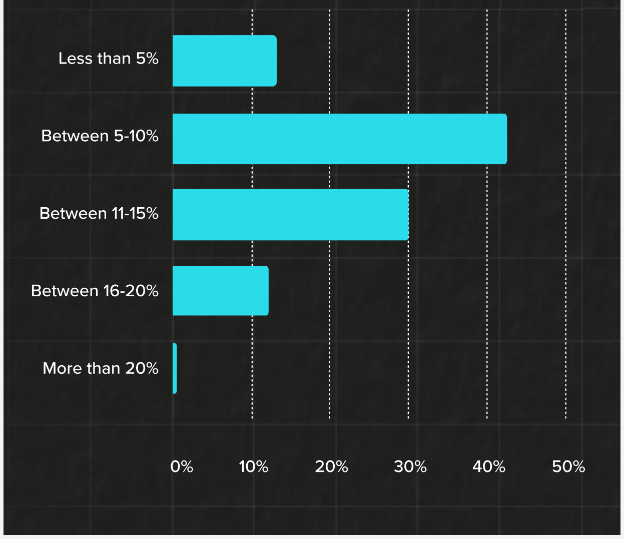


CYBERSECURITY SPENDING CONTINUES TO INCREASE AS BOARDS CHANGE THEIR ORGANIZATION’S CULTURE TOWARDS IT

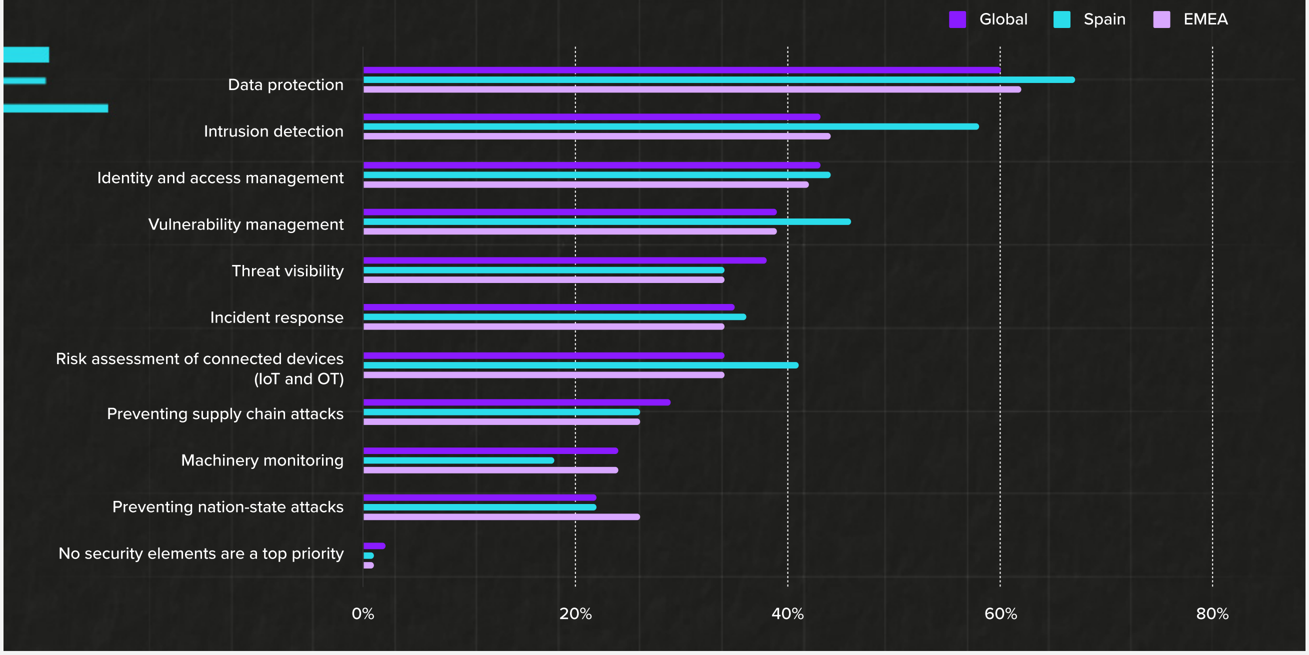
In an effort to mitigate risk, and followed by recent events such as the pandemic, Ukrainian war, etc. organizations are rethinking their cybersecurity spending. Just over three-quarters (77%) of Spanish IT professionals surveyed agree that the boards of directors are changing their organization’s culture towards cybersecurity in response to the threat of cyberwarfare. This is significant, as this oversight from the board has rarely been there before, and those individuals are now taking a shared responsibility in improving the cybersecurity posture of an organization.

In fact, more than 4 out of 5 (82%) of Spanish IT and security professionals surveyed agree that it’s somewhat likely (43%) or very likely (39%) that their company invests more of its budget into cybersecurity.

TO YOUR KNOWLEDGE, HOW MUCH OF YOUR ORGANIZATION’S IT BUDGET IS SPENT ON CYBERSECURITY?



WHEN ASKED TO SELECT SECURITY ELEMENTS IN ORDER OF TOP PRIORITY, THE FOLLOWING RESPONSE WAS RECEIVED

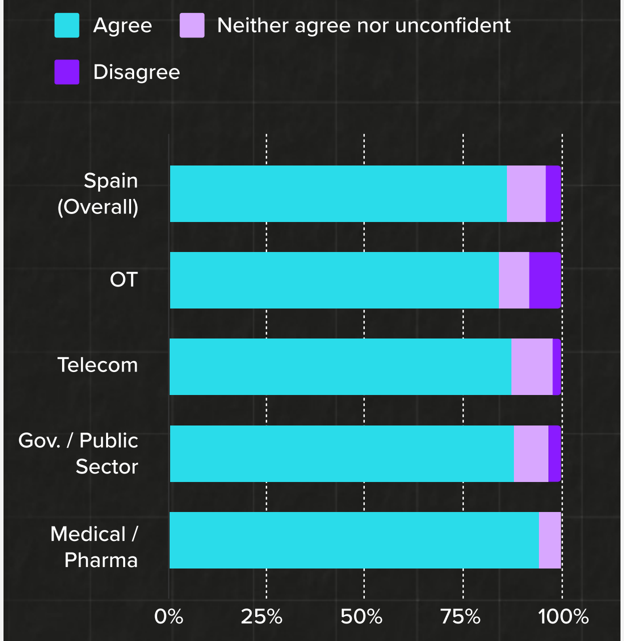


SECTORS AT RISK BUT READY TO RESPOND

While all industries are at risk for cyberattacks, critical infrastructure, healthcare, and government agencies stand out and pose attractive targets for nation-state actors. As Vesku Turtia, Regional Director of Armis Iberia, explains: "Nation-state actors continue to evolve in their activities, and critical infrastructure is becoming their main target in a cyberwarfare environment. The constant threats of targeted hacks on power grids, transportation systems, or water facilities are a top-of-mind going forward. In 2023, we expect to see more targeted ransomware and malware attacks and greater IT/OT convergence, making it imperative to have solutions designed to identify, monitor, and protect Industry 4.0 digital assets now and in the future."

Questioned about the readiness of their organizations to respond to cyber warfare threats, those were the answer of Spanish respondents:

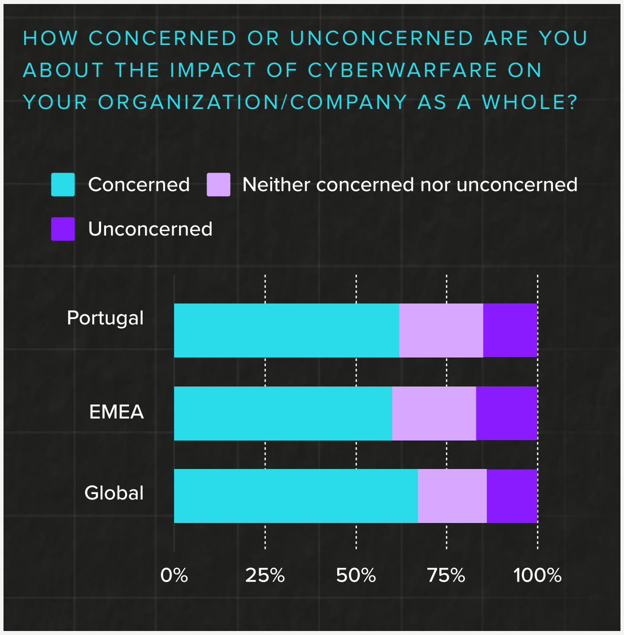
MY ORGANIZATION HAS PROGRAMS AND PRACTICES CURRENTLY IN PLACE SPECIFICALLY DESIGNED TO RESPOND TO CYBERWARFARE THREATS



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

CYBERWAR WORRIES PORTUGUESE COMPANIES, WHICH FEEL UNPREPARED TO DEAL WITH THE EVENT

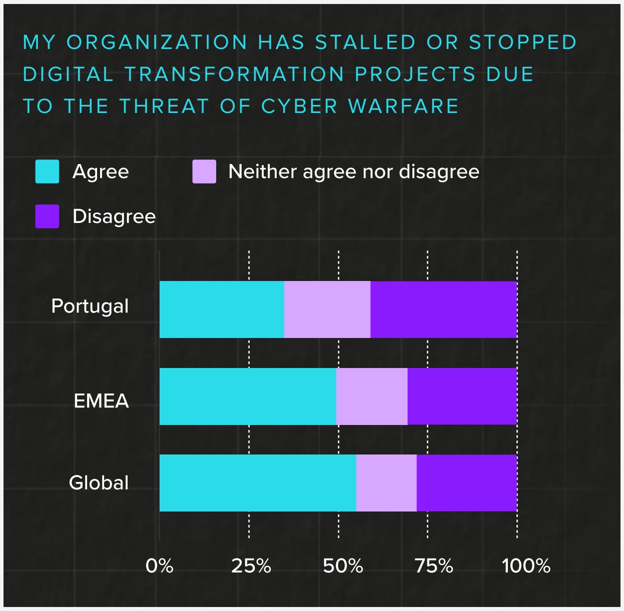
In Portugal, 62% of organizations are concerned about the impact of a cyberwar on their company as a whole. However, 38% of Portuguese companies are not yet taking this threat seriously, and 37% believe that their company is poorly prepared to deal with a cyberwarfare threat, a value higher than the European and global average (26% and 24%, respectively).


HOW CONCERNED OR UNCONCERNED ARE YOU ABOUT THE IMPACT OF CYBERWARFARE ON YOUR ORGANIZATION/COMPANY AS A WHOLE?

The current geopolitical situation has heightened concerns about possible cyberwar, with 67% of Portuguese respondents agreeing that the war in Ukraine has created a greater threat, slightly above the European and global averages (63% and 64%, respectively). Among the IT professionals surveyed, 31% said they experienced more threatening activity on their network between May and October 2022, compared to the previous six months. A figure above the European average (25%), but equal to that recorded globally (31%).

ONLY A FRACTION OF PORTUGUESE COMPANIES ARE HOLDING BACK ON THEIR DIGITAL TRANSFORMATION PROJECTS

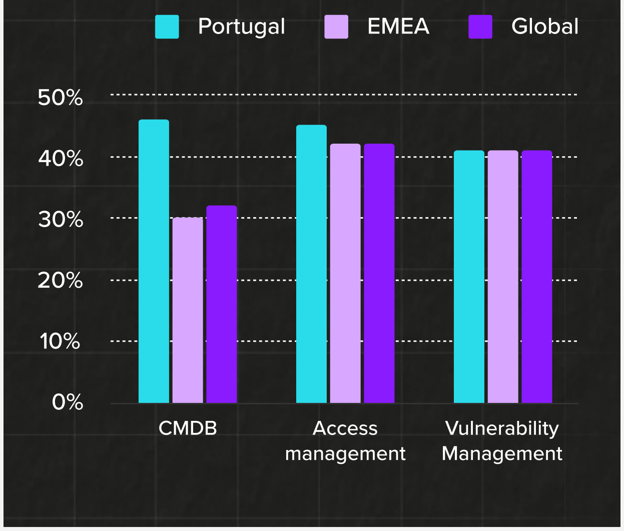
Despite increased concern over cyberwarfare, Portuguese companies remain focused on their digital transformation. Only 35% of the Portuguese IT professionals surveyed by Armis say that their organization has temporarily stopped or abandoned these projects, a figure significantly lower than the European (50%) and global (55%) averages.


MY ORGANIZATION HAS STALLED OR STOPPED DIGITAL TRANSFORMATION PROJECTS DUE TO THE THREAT OF CYBER WARFARE

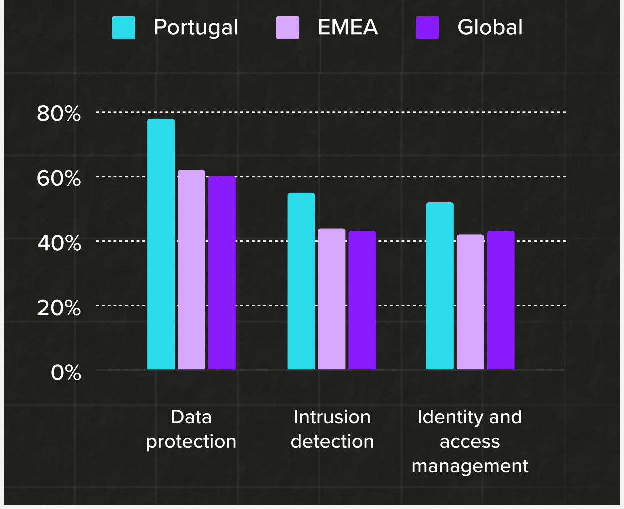
DATA PROTECTION IS A TOP PRIORITY AMONG PORTUGUESE PROFESSIONALS

The priority security elements for Portuguese IT professionals are data protection (78% of responses), intrusion detection (55%), and identity and access management (52%). As to which cybersecurity tools or services their organizations have increased investment in over the past six months, respondents indicate, Configuration Management Database (46%), followed by access management (45%) and vulnerability (41%). The top cybersecurity practices implemented in organizations are data backup (65%), the use of firewall and anti-malware software (64%), and encrypted data (57%).

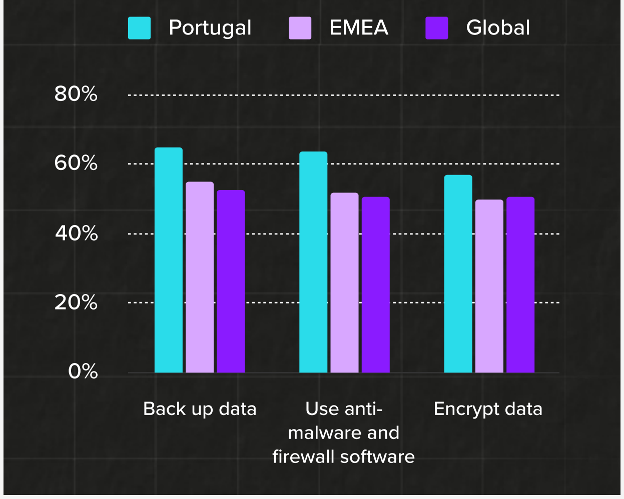
WHICH CYBERSECURITY TOOLS OR SERVICES, IF ANY, HAS YOUR ORGANIZATION'S INCREASED INVESTMENT IN WITHIN THE PAST SIX MONTHS?



WHICH SECURITY ELEMENTS, IF ANY, ARE A TOP PRIORITY? (SELECT ALL THAT APPLY)



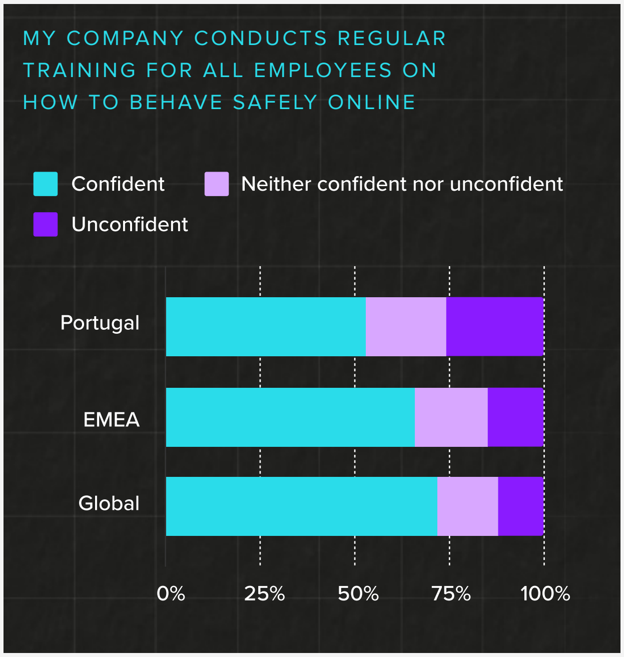
WHICH OF THE FOLLOWING CYBERSECURITY PRACTICES, IF ANY, IS IMPLEMENTED INTO YOUR COMPANY/ORGANIZATION?



ARMIS
SECURE VULNERABLE ASSETS
FOCUS ON HIGH-RISK VULNERABILITIES THAT CAN CAUSE COSTLY DISRUPTIONS
LEARN MORE

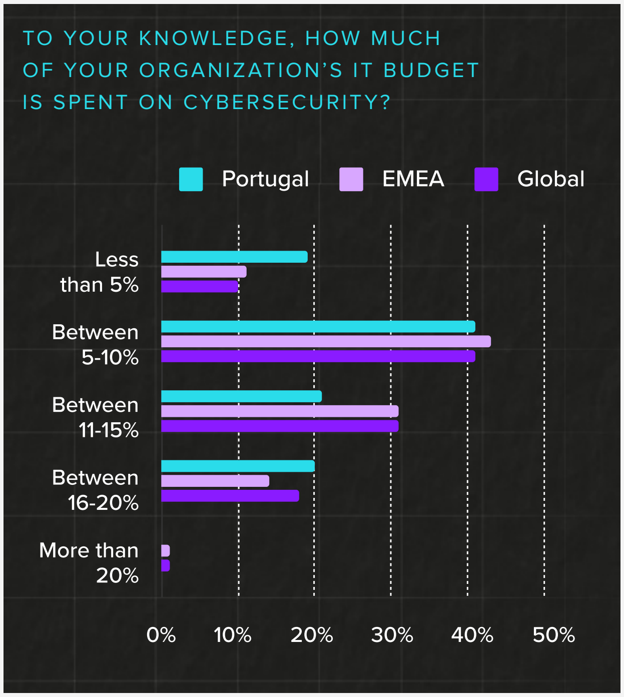
PORTUGUESE COMPANIES ARE INVESTING IN THE TRAINING OF THEIR EMPLOYEES REGARDING ONLINE SECURITY, BUT THERE ARE STILL EFFORTS TO BE MADE IN THIS AREA

Training has been another focus of Portuguese companies. Asked whether their company conducts regular training for all employees on how to behave safely online, 77% of IT professionals agreed.


MY COMPANY CONDUCTS REGULAR TRAINING FOR ALL EMPLOYEES ON HOW TO BEHAVE SAFELY ONLINE

MOST PORTUGUESE COMPANIES SHOULD INVEST MORE OF THEIR BUDGET IN CYBERSECURITY

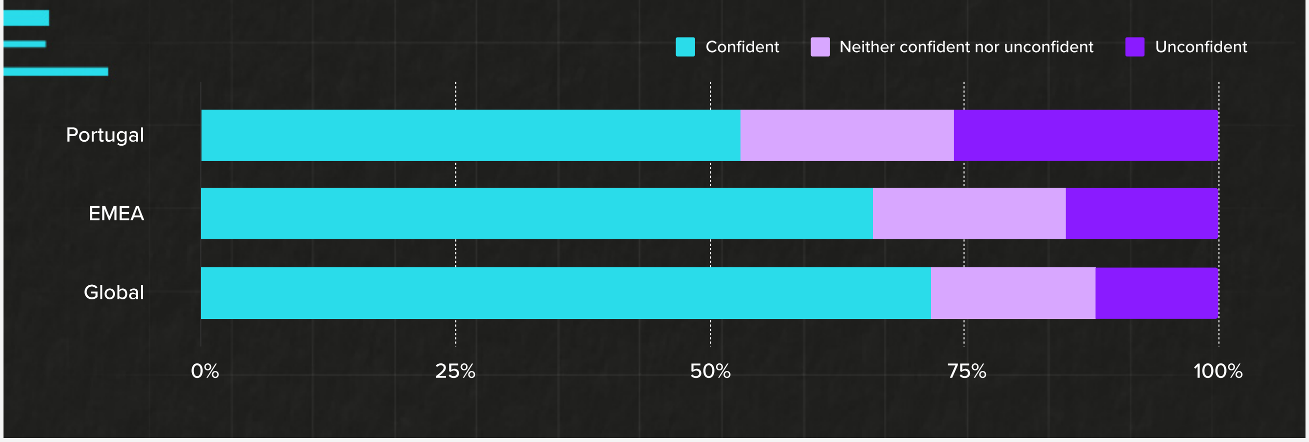
In light of recent events, such as the pandemic and the war in Ukraine, 78% of Portuguese respondents consider it likely that their organization will invest more of its budget in cybersecurity. Currently, a large proportion of the Portuguese companies only allocate between 5 and 10% of their IT budget to cybersecurity (41%).


TO YOUR KNOWLEDGE, HOW MUCH OF YOUR ORGANIZATION'S IT BUDGET IS SPENT ON CYBERSECURITY?

PORTUGUESE TRUST THE GOVERNMENT'S ABILITY TO DEFEND ITSELF FROM A CYBERFARWARE

When asked if they trust the government's ability to defend against cyberwarfare, 53% of Portuguese IT and security professionals expressed confidence. The Armis study also includes two specific questions for the Portuguese market, regarding the new Legal Regime for Cyberspace Security in Portugal. When asked whether the new regime has changed the way companies deal with cybersecurity measures, 53% of Portuguese IT and security professionals answered in the affirmative. Asked whether companies should be fined if they do not have security plans against cyber attacks, 67% of respondents answered 'yes'.

TO WHAT EXTENT ARE YOU CONFIDENT, IF AT ALL, THAT THE GOVERNMENT (OF THE COUNTRY WHERE YOU ARE BASED) CAN DEFEND AGAINST CYBERWARFARE?



WHY DO THESE FINDINGS MATTER?

The results of the Armis State of Cyberwarfare and Trends Report: 2022-2023 demonstrate organizations' growing concern about the increasing frequency and severity of cyberattacks, as well as the threat of cyberwarfare. The increasingly complex and sophisticated threat landscape is impacting diverse areas of business, across all industries. However, there is still a different pace and priorities in designing and adopting cybersecurity strategies.

> *"Cyberwarfare is the future of terrorism on steroids, providing a cost-effective and asymmetric method of attack that requires constant surveillance and expense to defend against," ... "Clandestine cyberwarfare is quickly becoming a thing of the past. Today, we are already seeing brazen cyberattacks by nation-states, often with the intention of gathering information, disrupting operations, or completely destroying data. Based on these trends, all organizations should consider themselves potential targets of cyberwarfare attacks and protect their assets accordingly."*
>
> **NADIR IZRAEL**
> CTO AND CO-FOUNDER AT ARMIS

> *"The current geopolitical instability, coupled with the Russian invasion of Ukraine, has also accelerated the increase in cyberattacks. Some sectors, fundamental to the economy and society, such as healthcare, critical infrastructure, and the industrial sector, are particularly at risk and it is paramount that all are protected."*
>
> *"Organizations in Iberia, which are still in a process of transformation and adaptation to new models of remote and hybrid work, will need to invest in cybersecurity to ensure that the adoption of new technologies can be done safely,"*
>
> **VESKU TURTIA**
> REGIONAL DIRECTOR, IBERIA, 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®