ARMIS®

THE STATE OF
CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

IDENTIFIES GLOBAL IT AND SECURITY PROFESSIONALS' SENTIMENTS ON CYBER SPENDING AND PREPAREDNESS

Respondents indicate organizations are unprepared to handle cyberwarfare, there's no one-size-fits-all response to ransomware, and cybersecurity spending is on the rise.

FOREWORD BY NADIR IZRAEL

CTO AND CO-FOUNDER, ARMIS

Armis is pleased to be able to share the results of our global cyberwarfare research study and market analysis with you. We hope that you find the contents of this global and its sister regional reports to be valuable and worthwhile.

Let us better consider the context that we are operating in today; **leading analysts[1]** predict that by 2025, cyber attackers will have weaponized operational technology (OT) environments to successfully harm or kill humans. While this may seem extreme, it underpins a trend in cyberwarfare as threat actors move from the reconnaissance and espionage realms into the kinetic application of cyberwarfare tools. These kinetic cyberweapons have already been discovered in the wild, although none specifically have been deployed to lethal effect. For example, the Triton malware discovered in 2017 **targeted and disabled[2]** safety instrumented system (SIS) controllers of a Saudi Arabian petrochemical plant which could have contributed to a plant-wide disaster had the problem not been identified. And in **February 2021[3]**, a hacker attempted to poison the water supply facility of a small U.S. city in the state of Florida via remote access. We have already seen ransomware attacks against the healthcare sector **result in human deaths[4]**, so the potential impact of cyberattacks - whether intentional or unintentional - is clear.

While kinetic cyber threats are the future of the cyber arms race, cyberweapons are hardly a new concept. The world got a peek into the **National Security Agency's[5]** (NSA) cyber arsenal in 2016 with the **Shadow Brokers leaks[6]**, which exposed some of the most powerful and invisible cyberweapons on earth. This leaked cyber arsenal, which included the EternalBlue vulnerability, became the basis of some of the most extensive compromises in history, including NotPetya and WannaCry.

The development of these cyberweapons has also accelerated an entire industry known as the zero-day market, a shadowy collection of researchers, brokers, and websites dedicated to profiting from zero-day exploits. While no one knows the exact dollar amount of the industry as a whole, openly published price lists have revealed the price of a working zero-click exploit as **$2.5 million and $2 million for Android and iOS[7]**, respectively.

The landscape here continues to evolve significantly and has changed monumentally over the last five years, especially following Russia's invasion of Ukraine in February 2022. As such, business and IT leaders must understand the evolving threat landscape so that they can improve their cybersecurity posture to defend against these attacks, which is why we've created the **Armis State of Cyberwarfare and Trends Report: 2022-2023**. To prepare this report, Armis commissioned a proprietary study surveying 6,021 IT and security professionals in firms with more than one hundred employees across the USA, UK, Spain, Portugal, France, Italy, Germany, Austria, Switzerland, Australia, Singapore, Japan, the Netherlands, and Denmark. In addition, Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Questions asked of respondents included the likes of:

- Would you consider your organization prepared to handle cyberwarfare?
- To what extent are you confident, if at all, that the government of the country where you are based can defend against cyberwarfare?
- What is your organization's policy of paying ransoms in the event of a ransomware attack?
- Which cybersecurity practices are implemented in your organization?

The responses to these and other questions were used to determine the sentiment of IT and security professionals globally, regionally, and country-by-country on a case-by-case basis to report on the following trends. Let's take a closer look at the findings and how they relate to how organizations can improve their cybersecurity posture to defend against cyberwarfare attacks.

CYBERWARFARE

/ˈsʌɪbəˌwɔːfɛː/

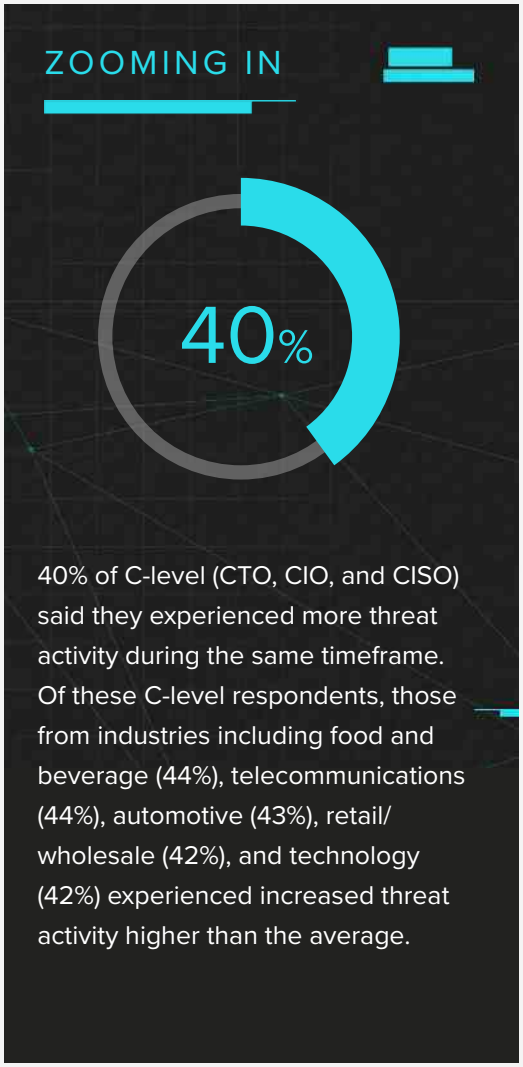
NOUN:

The use of cyberattacks, causing comparable harm to actual warfare and/or disrupting vital systems or services. Some intended outcomes could be espionage, sabotage, propaganda, manipulation of public opinion, intimidation, or disruption of critical services.

TABLE OF CONTENTS

ARE ORGANIZATIONS PREPARED TO WEATHER THE STORM THAT IS CYBERWARFARE?

Key findings from the global report.



According to the Armis study, one-third (33%) of global organizations are not taking the threat of cyberwarfare seriously. These organizations identify as indifferent or unconcerned about the impact of cyberwarfare on their organizations as a whole, leaving room for security gaps. And, growing geopolitical tensions resulting from the war in Ukraine have made the threat of a cyberwarfare attack far more plausible. More than 64% of IT and security professionals surveyed by Armis agree that the war in Ukraine has created a greater threat of cyberwarfare, and more than half (54%) of respondents who are the sole decision maker for IT security said they experienced more threat activity on their network between May and October 2022 when compared to the six months prior. Given this, it's no surprise that 45% of respondents say that they have had to report an act of cyberwarfare to the authorities.

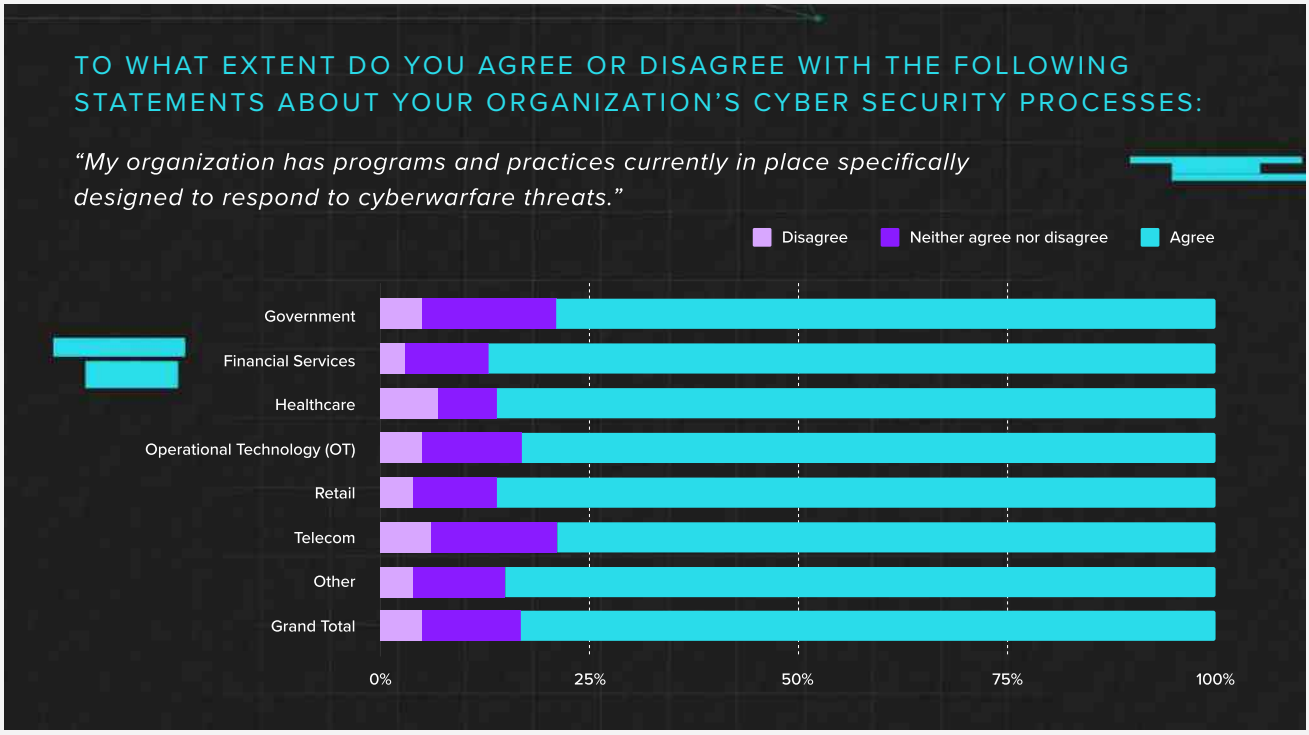
C-LEVEL RESPONDENTS:

Have you experienced more or less threat activity, if any, on your network in the past six months than the six months prior?

VERTICALS	INDUSTRY SECTOR	MORE	SAME	LESS	N/A	I DON'T KNOW
Government	Government, Local Authority, Public Sector Agency	**39%**	44%	14%	3%	
Financial Services	Financial Services and Insurance	**20%**	70%	10%		
Healthcare	Medical, Healthcare, Pharmaceutical	**26%**	52%	20%	2%	
Operational Technology (OT)	Automotive	**43%**	33%	24%		
	Distribution, Logistics, Transport	**30%**	48%	19%	4%	
	Food & Beverage	**44%**	44%	11%		
	Manufacturing, Engineering,	**40%**	30%	8%	22%	
	Oil, Gas, Mining, Construction, Agriculture	**30%**	50%	15%	5%	
	Transportation	**32%**	36%	18%	14%	
	Utilities: Energy and Water	**15%**	62%	15%	8%	
OT Total		**37%**	35%	12%	16%	
Other	Charity, Not-for-profit	**29%**	29%	14%	29%	
	Other (Please specify)	**33%**	43%	5%	10%	10%
	Technology	**42%**	25%	30%	2%	1%
Other Total		**42%**	25%	29%	2%	1%
Retail	Retail/Wholesale Services	**42%**	40%	15%	3%	
Telecom	Telecommunications, Cable, Satellite	**44%**	38%	18%		
Grand Total		**40%**	31%	22%	6%	0.5%

Proprietary data from the Armis Asset Intelligence and Security Platform collected June 1, 2022 through November 30, 2022 confirmed the aforementioned trends 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.

The worsening threat landscape has tangibly impacted digital transformation projects globally, slowing innovation worldwide. Over half (55%) of respondents surveyed say that their organizations have stalled or stopped digital transformation projects due to these threats. This percentage is even higher in specific countries, including Australia (79%), the USA (67%), Singapore (63%), the UK (57%), and Denmark (56%).



While all industries are at risk for cyberattacks, critical infrastructure, healthcare, and government agencies stand out and pose attractive targets for nation-state actors. Healthcare is attractive due to the breadth of the attack surface and the effect an attack can have on critical processes and patient health and safety. Government agencies are attractive because of the data that they store, and critical infrastructure continues to be a high priority, given its importance to national and economic security.

With anxiety about the growing cyberwarfare threat and the average cost of a data breach in the U.S. at **$9.44 million USD**[8] and $4.35 million USD globally, it is no wonder industry analysts are **projecting**[9] that worldwide spending on security and risk management will grow by 11.3% in 2023. Remote and hybrid work models, the transition from virtual private networks (VPNs) to zero trust network access (ZTNA), and the shift to cloud-based delivery are all contributing factors, but what this really boils down

to is an ever-expanding attack surface coupled with a preponderance of countries able to develop sophisticated cyber weapons. At the end of the day, can digitized and truly connected organizations afford not to increase cyber spending?

Despite the risk of cyberwarfare impacting an organization, cyber defense and resilience against such attacks remain low. More and more nation-states have moved their focus away from critical infrastructure to attacking commercial entities of all shapes and sizes. Ironically, this research found that nearly a quarter (24%) of global organizations feel unprepared to handle the cyberwarfare threat, and yet the lowest-ranked security element among IT and security professionals is preventing a nation-state attack. Furthermore, even for organizations willing to spend the money on a robust cybersecurity program (we'll get more into spending trends later on!), finding the people to fulfill cybersecurity roles with the skills needed to effectively monitor related technologies and software continues to be an issue. The number of unfilled cybersecurity jobs worldwide **grew 350%**[10] between 2013 and 2021, from one million to 3.5 million. It's predicted that in 2025 the same number of jobs will still be open.

WHAT INDUSTRIES ARE MOST VULNERABLE?

THREATS TO CRITICAL INFRASTRUCTURE

With the prolonged conflict in Ukraine, 2022 has seen international agencies issuing multiple alerts about malicious Russian cyber operations targeting critical infrastructure. Of note, Industroyer2 and InController/PipeDream are modular attack tools intended for Operational Technologies (OT) throughout all industries and include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), Remote Terminal Units (RTUs), and programmable logic controllers (PLCs) operational environments.

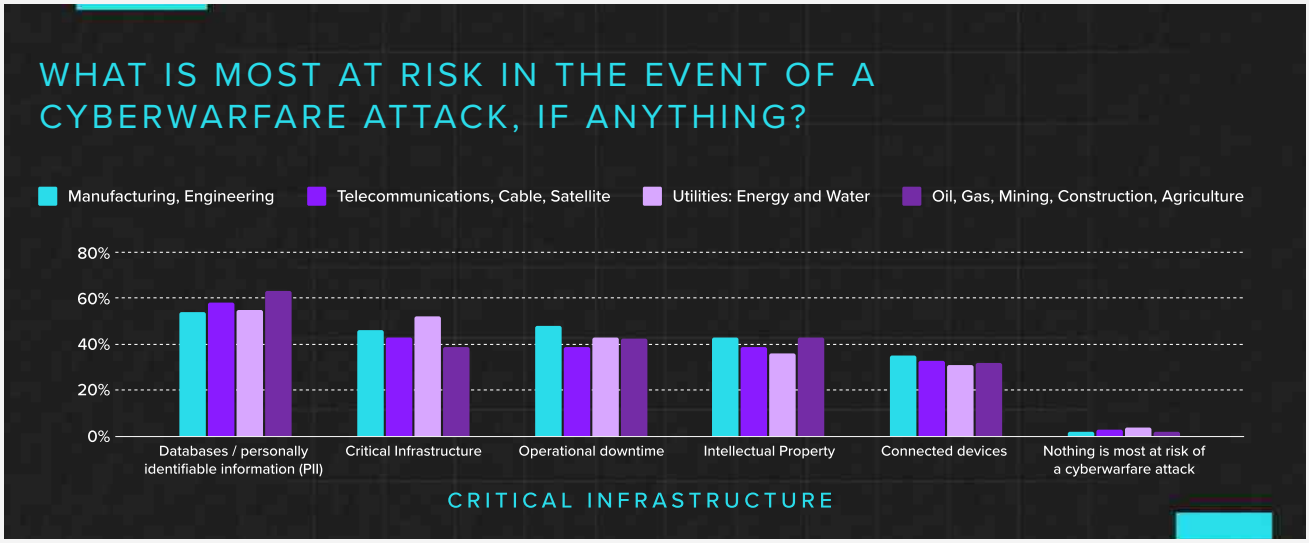
In May 2021, the **Colonial Pipeline**[11], which controls nearly half the gasoline, jet fuel, and diesel flowing along the East Coast of the U.S., became the victim of a ransomware attack within IT, affecting its OT operations. The Colonial Pipeline hack is the largest publicly disclosed cyberattack against critical infrastructure in the U.S. to date. After conferring with the Federal Bureau of Investigation (FBI), the U.S. Department of Energy (DOE), the Department of Homeland Security (DHS), and Cybersecurity and Infrastructure Security Agency (CISA), Colonial Pipeline made the difficult decision to pay the cryptocurrency ransom demanded by the DarkSide hackers.

The company felt that paying to get the decryption key was the best way to swiftly and securely get the pipeline back up and running. Roughly one month later the FBI was able to recapture the majority of the ransom payment by seizing Bitcoins belonging to the hackers.

Nation-state cyberwarfare is not limited to adjacent neighbors or active conflict participants. Aggressors may target other countries for any number of reasons, related (for example, supplying arms) or unrelated to the conflict. In 2021, the U.S. formally accused Nobelium, a state actor of Russia's Foreign Intelligence Services, of carrying out the SolarWinds hack to infiltrate U.S. and EU government networks. The Nobelium attack altered the threat landscape for virtually every industry. In October of 2022, the pro-Russia hacker group Killnet launched **dozens of DDoS attacks**[12] against the U.S. aviation industry and proclaimed all U.S. critical infrastructure should be under persistent attack.

The news of these continued and escalating cyberwarfare attacks, plus the efforts of public and private organizations to raise awareness, have not been ignored by business leaders. The Armis State of Cyberwarfare and Trends Report: 2022-2023 found that 74% of global respondents responsible for critical OT infrastructure surveyed agree that boards of directors are changing the organizational culture towards cybersecurity in response to the threat from cyberwarfare.

When looking at the industries most commonly associated with critical infrastructure (see table below), the convergence of IT and operational technology (OT) in Industry 4.0 is apparent from the responses. Respondents were asked to select up to three items most at risk in the event of a cyberwarfare attack. In each sector, databases and personally identifiable information (PII) were ranked as the greatest concern. Critical infrastructure (physical equipment and facilities), operational downtime, and intellectual property rounded out the midrange of at-risk areas, with connected devices coming as the lowest concern across critical infrastructure sectors.



These responses indicate a range of concerns across IT, OT, and Industrial Control Systems (ICS) environments, which is not surprising given the recent and rapid convergence of these once disparate systems. Many ICS and OT systems in critical infrastructures were built decades ago and are still secured largely through legacy methods based on network design and role-based access. As these environments become more interconnected and automated, the attack surface expands at the intersection of existing networks and assets that were never intended to connect to those networks.

This intersection of connected assets is what drives Armis to conduct security vulnerability research to help spread awareness of vulnerabilities and attacks impacting critical infrastructure. In March 2022, the Armis research team publicly disclosed three zero-day vulnerabilities potentially impacting more than 20 million APC Smart Uninterruptible Power Supply (UPS) devices, which provide emergency backup power for mission-critical assets in data centers, industrial facilities, hospitals, and more. These vulnerabilities, collectively known as TLStorm, allow threat actors to disable, disrupt, and destroy these UPS devices and attached assets. Exploiting these vulnerabilities can allow an attacker to weaponize UPS devices, for instance, by tampering with the voltage to the point they start burning and go up in smoke. These vulnerabilities occur in cyber-physical systems that bridge our digital and physical worlds. As such, they're even more critical to identify, as they give cyberattacks the possibility of real-world, life-threatening consequences and/or can result in the physical destruction of the targeted infrastructure.

THREATS TO HEALTHCARE

The healthcare sector is of critical importance to citizens of every nation. It is vital to how any society functions and plays a pivotal role in the development of any modern state. Due to the real-world, life-threatening consequences when patient safety is in jeopardy, healthcare continues to be a top target of malicious actors. For instance, in October 2022, **CommonSpirit Health**[13] suffered a major ransomware attack on a system that runs 140 hospitals and more than 1,000 care sites throughout the United States. As of late 2022, this attack was still affecting almost 20 million Americans across 21 states, and as a result, healthcare workers were providing care without the medical records of their patients. This, of course, is a very dangerous way to administer healthcare. In one such incident, a three-year-old in Iowa received and luckily survived a "megadose" of pain medication as a result of this attack. Earlier in 2020, a much smaller **cyberattack on a German hospital in Duesseldorf**[14] resulted in a network outage and patients needing to be rerouted to other hospitals, resulting in the death of one patient.

Not only are healthcare attacks life-threatening, but they are extremely costly to healthcare systems that are already working on strained budgets and are still trying to recover from the surge of the COVID-19 pandemic. **Healthcare CIOs**[15] are struggling to retain key tech and security talent as remote workers pursue the higher incomes available in other sectors. This reduction in trained staff comes at a critical time for healthcare organizations, as they remain one of the most targeted sectors of cyberwarfare and cybercrime. (IBM currently estimates the average cost of a healthcare breach at **$10.1 million USD**[16], higher than the $9.44M estimated for all industries.) When Ireland's **Health Service Executive**[17] was attacked by Conti ransomware in 2021, the publicly-funded healthcare system was forced to move to paper-based processes, leading to the cancelation of 80% of patient appointments and an estimated total cost of $600 million USD for remediation and replacement of systems.

According to this study, 72% of respondents responsible for IT in healthcare, medical, and pharmaceutical environments agree that their boards of directors are changing their organization's culture towards cybersecurity in response to the threat of cyberwarfare. This trend is driven by the prevalence and steady cadence of cyberattacks on the healthcare sector: 45% of industry respondents indicated they've seen the same amount of threat activity on their network between May and October 2022 when compared to the six months prior, while 28% said they've experienced more threat

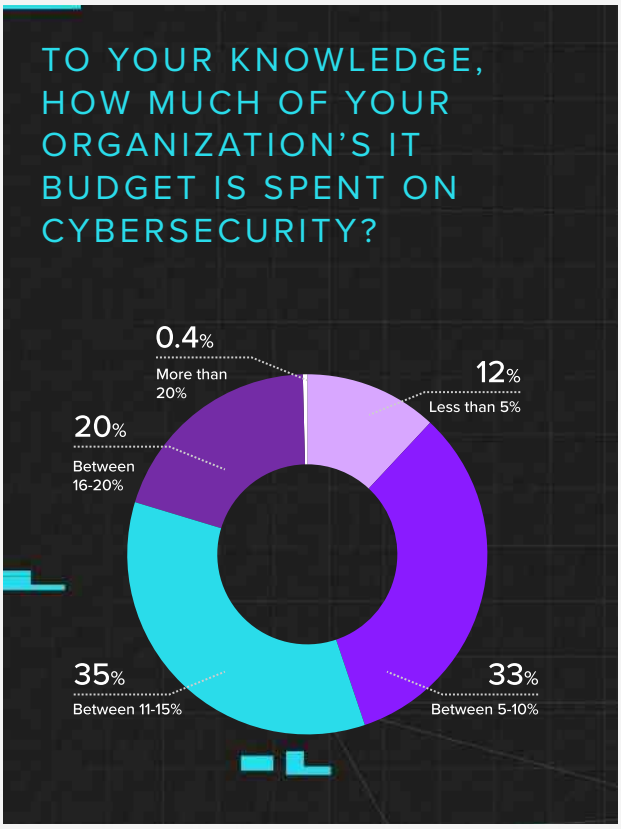
ZOOMING IN

Global healthcare organizations surveyed by Armis indicated their policy on paying ransoms in the event of a ransomware attack is that they:

activity when evaluating the same timeframes. And, respondents indicated they are somewhat or very concerned about the impact of cyberwarfare on their organizations as a whole (70%), their company's critical infrastructure (72%), and their company's services (68%).

Even still, cybersecurity spending among healthcare organizations is on the low end when compared to other industries globally. Nearly half (45%) of healthcare companies spend less than 10% of their IT budgets on cybersecurity. On average, global healthcare respondents indicated they spend around 11% of their company's IT budget on cybersecurity, with some spending 11-15% (35%) or 16-20% (20%), and few spending 20% or more (less than 1%).

As healthcare IT continues to advance and digitize patient care, innovation has the potential to address some of the major challenges facing the healthcare industry, such as staffing shortages, rising costs, and compliance issues. However, 55% of respondents stated that the threat of cyberwarfare has the potential to slow down this digitization process. This can have a significant impact on patient lives, as the full benefit of digitization may not be realized if it is slowed down by cyberattacks. If digitization is not fully embraced with cybersecurity at the forefront, these new projects could be exploited. Take pneumatic tube systems (PTS), for instance. These systems are used in over **80% of hospitals in North America**[18] and installed in more than 3,000 hospitals



worldwide, automating logistics and transport of materials throughout hospitals via a network of pneumatic tubes. These systems play a crucial role in patient care and are utilized nearly 100% of the time. Armis researchers identified nine vulnerabilities in these devices back in 2021, dubbed PwnedPiper, which if targeted by cybercriminals, could enable an unauthenticated attacker to take over complete control of a targeted hospital to deploy a sophisticated ransomware attack or leak sensitive hospital information.

THREATS TO GOVERNMENT AGENCIES

Assets are the common denominator in our modern, global, and ever-fragmented digital world. And no one entity has more assets (people, devices, or software) than government agencies and the people they seek to serve and protect. Despite what's happened in recent years, global respondents from the public sector are seemingly confident when it comes to handling cyberwarfare:

Perhaps this increased confidence comes from additional knowledge sharing amongst global alliances. **The Five Eye[19]** nations (Australia, Canada, New Zealand, the UK, and the U.S.), are now proactively sharing intelligence resources to strengthen their overall security posture, particularly when it comes to protecting assets. And more interestingly, should any of these counties be drawn into a cyberwar conflict, 63% of global respondents said they would support conscription into a cyber defense league.

This overwhelming display of agency confidence is highlighted again, as this survey found that 9 in 10 (90%) government respondents are confident that their country's home nation can protect against cyberwarfare. However, once breaches are detected, 55% of global respondents believe their government agencies are unable to cope with and ultimately remediate the negative impacts of cybercriminals. This could not have been more true in April 2022 when attackers from the Russian ransomware group known as Conti **overtook the Costa Rican government[20]**. Their brazen attack left the tax systems of the subtropical country frozen, reacting havoc on exports and delaying payments to native workers. Throughout the attack, Conti managed to leak **97% of all the stolen data[21]**. By May 2022, the situation had deteriorated, requiring the Costa Rican government to declare a state of emergency.

In the United States, government agencies, institutions, and educational systems have felt the global trickle-down effect cyberwarfare groups. During the height of the 2020 pandemic in the United States, 79 ransomware attacks were made against government agencies. It is estimated that these agencies lost approximately **$18.8 billion[22]** in recovery costs and downtime. As a result, the U.S. government launched an aggressive mission in Q3 2021 to reduce the overall volume of ransomware with **StopRansomware.gov[23]**. It is the hope that with public-private partnerships, government agencies, such as those in the United States, can begin to better protect, detect, and remediate the impacts of ransomware.

ZOOMING IN

Government organizations are the least likely out of any industry to pay a ransom in the event of a ransomware attack, with 43% of respondents saying their organization's policy is to never pay (significantly higher than the global average (26%) of respondents whose organization's have policies to never pay).

WHAT CYBERSECURITY TRENDS ARE HAPPENING WORLDWIDE?

THERE'S NO ONE-SIZE-FITS-ALL RESPONSE TO RANSOMWARE

Many mistake ransomware attacks as efforts sheerly intended to steal critical data. The truth is, however, that most organizations are easy targets and cybercriminals are opportunists. After all, it's much more efficient and profitable to extort these businesses into paying a multi-million dollar ransom to regain access to their operations than it is to exfiltrate and sell hundreds of thousands of individual pieces of data on the black market.

Whether it is nation-state actors or cybercriminals deploying the ransomware, the anatomy of a ransomware attack is relatively the same. The attack begins with ingress which often takes the form of delivery through a compromised website, phishing, or a targeted attack. Once inside, the attackers move laterally through the network, escalating privileges and burrowing into the network. Through the use of tunneling, the attackers establish a command and control connection which eventually leads to the exfiltration of an organization's data and the launching of the ransomware which will encrypt that data on the target system.

DarkSide is a group of Eastern European cybercriminals that developed REvil, a ransomware tool that originally began as the GandCrab variant and is one of the best-known ransomware-as-a-service (RaaS) platforms thanks to the previously mentioned Colonial Pipeline attack of 2021. It first appeared in April 2019 and was at the height of its activity until October 2021, when REvil servers were hacked in a multi-country operation and forced offline. Until this point, DarkSide provided its malware to "affiliates" and split the ransom with the clients conducting the attacks. In addition to the malware itself, DarkSide provided the decryption mechanism (which is still considered one of the most sophisticated decryption systems of any of the malware families), infrastructure for darknet chats,

ZOOMING IN

Who pays, who doesn't?

Just over 3 in 10 (31%) IT professionals surveyed in a company with more than 500 employees said their organization's policy on paying ransoms in the event of a ransomware attack is that they never pay, whereas over a fifth (23%) of IT professionals surveyed in a company with 100-249 employees said the same. These responses differ when comparing countries side-by-side: nearly half (47%) of IT professionals surveyed in the USA said their organization's policy on paying ransoms in the event of a ransomware attack is they always pay, compared to 1 in 14 (7%) in Japan who said the same.

darknet leak sites, and money laundering services. With the help of initial access brokers, which is an emerging breed of cybercriminals that sell access to a compromised network, affiliates gain access to a target network, launch the REvil payload, and negotiate with the affected organization for a ransom to restore the encrypted data.

If the proliferation of ransomware and the zero-day market wasn't enough, Interpol Secretary General Jurgen Stock stated in May 2022 that he is concerned that state-developed cyber weapons will become available on the darknet in the next couple of years. "That is a major concern in the physical world — weapons that are used on the battlefield and tomorrow will be used by organized crime groups," Stock said during a **CNBC-moderated[24]** panel at the World Economic Forum in Davos, Switzerland.

When respondents were asked for this survey about their organization's policy on paying ransoms in the event of a ransomware attack, IT professionals globally were divided in their responses. Twenty-four percent of respondents indicated their organization always pays, 31% said their organization only pays when customer data is at risk, 26% said the organization never pays, and 19% indicated that it depends.

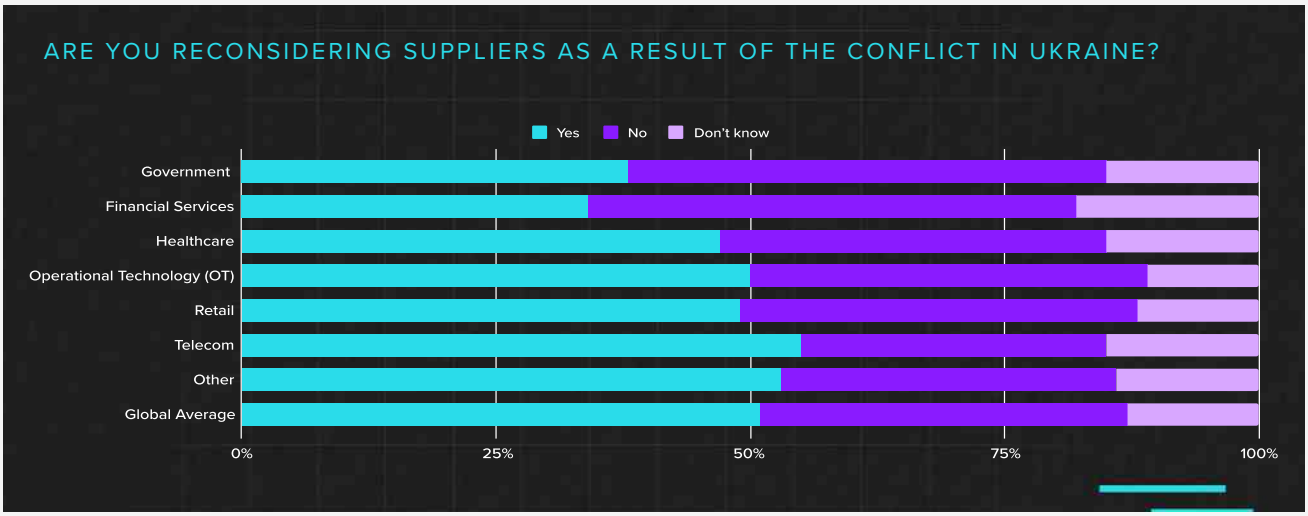
CYBERSECURITY SPENDING CONTINUES TO INCREASE

If you are seeking indications of where firms will be spending their IT dollars, then you won't be surprised to learn that firms will be increasing their spending on related cyber defense, resilience, and protection services.

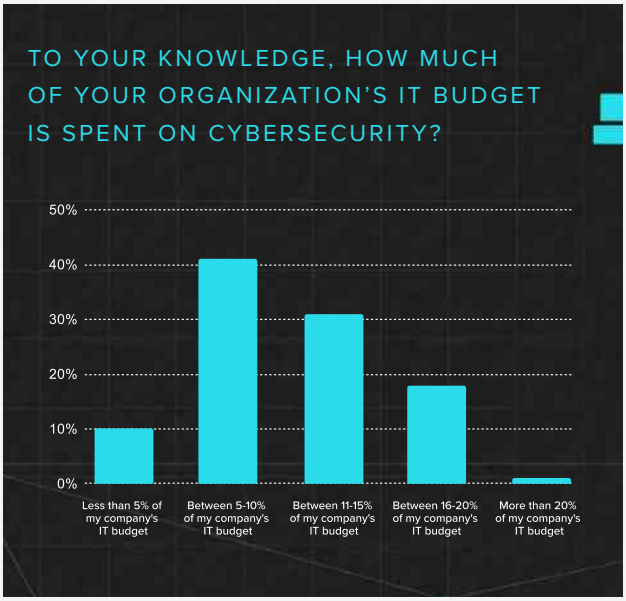
Just over three-quarters (76%) of IT professionals surveyed agree that the boards of directors are changing their organization's culture towards cybersecurity in response to the threat of cyberwarfare. This is significant, as this oversight from the board has rarely been there before, and those individuals are now taking a shared responsibility in improving the cybersecurity posture of an organization.

With this, just over half (51%) of global respondents said they were reconsidering suppliers as a result of the Ukrainian conflict and that they foresee their organization onboarding new cybersecurity provider(s) or Managed Security Service Providers (MSSPs) immediately (31%) or over the next six months (29%). It's critical that vendors are aware of spending trends and where organizations are most in need of their services so that they can ensure they're delivering the right solutions.

> *"The skills shortage in cybersecurity is still a massive issue as lack of headcount increases the demand for services or solution wraps, playing very well into partner value capabilities. The skills shortage makes the market strong in cybersecurity, especially for MSSPs and those partners looking to reduce their business impact risks by developing in-house services for better returns."*
>
> **TIM MACKIE**
> VP WORLDWIDE CHANNEL AT ARMIS

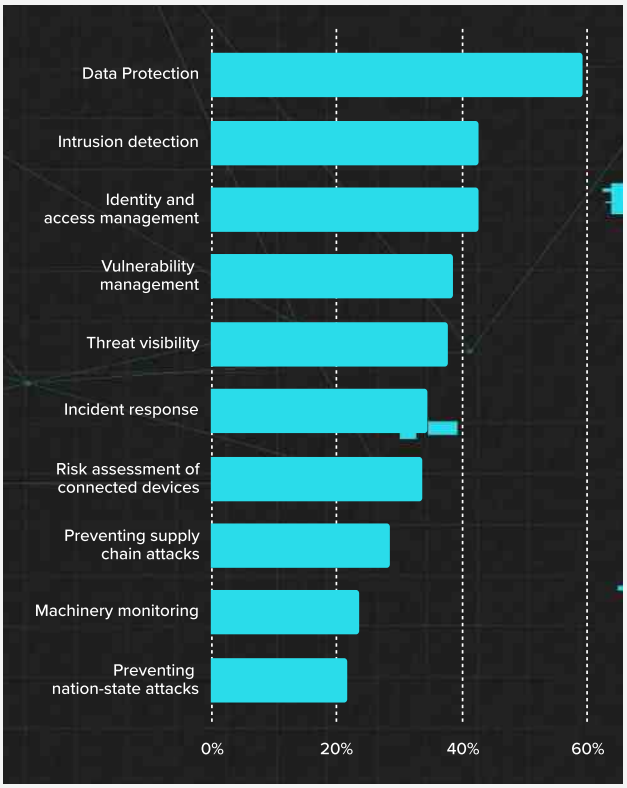


Looking at the data, almost 4 in 5 (78%) IT professionals surveyed said, when thinking about recent and ongoing sudden global events (such as the pandemic, Ukraine conflict, etc.), it's likely that their company invests more of its budget into cybersecurity, with nearly 2 in 5 (37%) who think it's very likely. So, how much are organizations spending, and what are they spending on? This survey found that globally, the average percentage of IT budgets allocated towards cybersecurity is 11%, further breaking down as follows:



For those that spend the most, 37% said they are very likely to increase investment soon, and 41% somewhat likely. However, companies that have fewer investments are less likely to increase their spending soon.

When asked to select security elements in order of top priority, the following response was received globally:



More than 2 in 5 (42%) IT professionals surveyed foresee their organization investing in **vulnerability management** immediately, while almost 3 in 10 (28%) said within six months. Regarding investments in **asset management**, 37% of respondents indicated their companies would make investments immediately, and 30% said they would invest within six months.

Not only are businesses investing in cybersecurity solutions, but they're also adopting cybersecurity-first principles organization-wide and investing in cybersecurity training. One-third (33%) of IT professionals surveyed foresee their organizations adopting **"zero trust"** models immediately, while 28% said within six months. When it comes to cybersecurity training, 41% of global respondents indicated their organizations will invest in increased cybersecurity training immediately, while 46% said they'll invest over the next year. Only 4% of organizations said that they will not take any action to increase cybersecurity training.

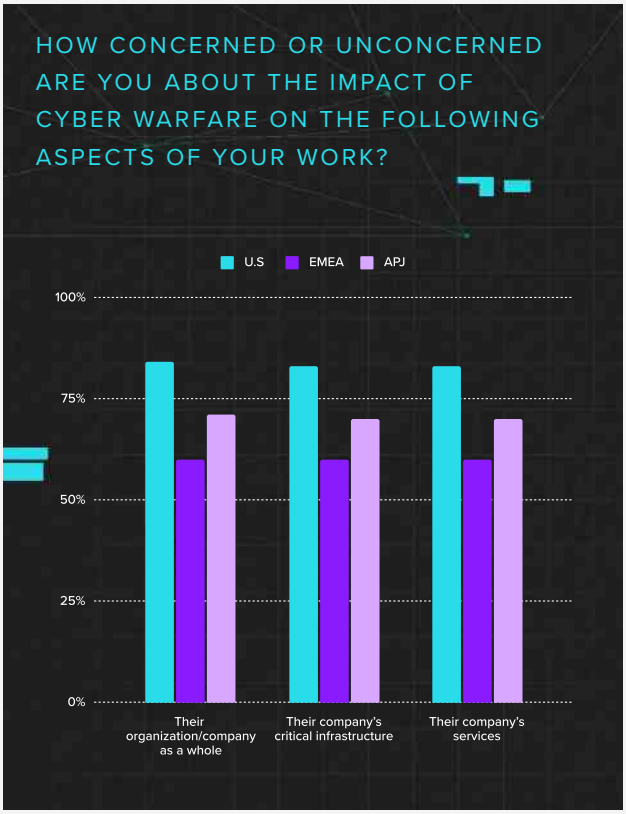
> *"Security teams have a distinct need for a high degree of contextualized visibility into the entire technology operating landscape to perform effectively. The level of visibility offered to security teams using modern technologies is helping CISOs and their teams identify true, business-contextual, data-proven opportunities to eliminate older, competing solutions and all related expenses from the environment."*
>
> **CURTIS SIMPSON**
> CHIEF INFORMATION SECURITY OFFICER (CISO) AT ARMIS

WHAT REGIONAL (U.S., EMEA, AND APJ) DIFFERENCES STAND OUT?

In addition to the global trends highlighted above, regional differences also stood out when grouping responses from the U.S., EMEA, and APJ (Australia, Japan, Singapore). For example:

CONCERNS ABOUT THE IMPACT OF CYBERWARFARE

Respondents from the U.S., EMEA, and APJ were asked how concerned or unconcerned they are about the impact of cyberwarfare on various aspects of their work. Respondents from EMEA indicated less concern when compared to their APJ counterparts who are more concerned, and significantly less concern when compared to U.S. IT pros who have the highest level of concern.



THREAT ACTIVITY AND THE NUMBER OF BREACHES EXPERIENCED

- Respondents from APJ have experienced the least number of cybersecurity breaches according to this survey, with 53% of APJ respondents indicating their company has experienced one or more cybersecurity breaches. Comparatively, almost 3 in 5 (58%) respondents in EMEA and 7 in 10 (73%) U.S. respondents indicated that their organizations experienced one or more cybersecurity breaches.
- U.S. organizations have also experienced the highest amount of increased threat activity over recent months (45%) when compared to their APJ (36%) and EMEA (25%) counterparts.

CONFIDENCE IN ORGANIZATIONAL PREPAREDNESS

Respondents from the U.S. are the most confident that their company has allocated a sufficient budget for cybersecurity programs, people, and processes, with almost 9 in 10 (88%) respondents expressing confidence in the U.S. as compared to 78% in APJ and 76% in EMEA. Further, 90% of U.S. respondents indicated that employees from their organizations know who to speak to if they notice suspicious cyber activity, compared to 4 in 5 (82%) for those based in EMEA or APJ.

CYBERSECURITY PRACTICES THAT HAVE ALREADY BEEN IMPLEMENTED

- When it comes to investing in cybersecurity insurance, U.S. companies are most likely to have invested (45%), followed by APJ (37%), and EMEA (31%).
- When it comes to the importance of educating employees, all three regions shared similar responses: USA (51%), EMEA (49%), and APJ (45%).
- In regard to creating a security-focused work culture, 44% of U.S. respondents indicated their company has a culture with security top-of-mind when compared to 37% of respondents in EMEA and 33% in APJ.
- The U.S. is the most likely to have a Cyber Risk Framework implemented (43%), while 34% of respondents from APJ have a framework implemented, and 31% of EMEA respondents have a framework.

SECURING SENSITIVE DATA & SMART WORKING

Respondents were asked whether they agree or disagree with a list of statements:

- *"My organization holds sensitive data, there are regulations we have to follow, and we want to minimize any negative effect from a security event."*
  - » Of those that agreed: 91% U.S., 84% APJ, and 83% EMEA.
- *"The issue of IT security has become more important to employees with the adoption of smart working."*
  - » Of those that agreed: 91% U.S., 85% APJ, 81% EMEA.

COUNTRY-BY-COUNTRY ANALYSIS

For those who'd like to take a deeper dive into the regional differences highlighted above, the Armis team has prepared unique country-by-country analysis most relevant to the nations and territories surveyed as part of this report.

To read those individual country reports, which you can access in English as well as some translated versions, go to https://www.armis.com/cyberwarfare.

1. **USA**
2. **UK**
3. **France**
4. **DACH** (Austria, Switzerland, Germany)
5. **Iberia**
6. **Italy**
7. **Denmark**
8. **Netherlands**
9. **APJ** (Australia, Japan, Singapore)

CONCLUSION

Why do these findings matter and what can your organization do to protect itself?

Global IT and security leaders admit that they are not taking the threat of cyberwarfare seriously, that they feel underprepared to handle cyberwarfare, and that the lowest-ranking security element in their eyes is preventing nation-state attacks. To add, they're seeing more threats of cyberwarfare as a result of the war in Ukraine, which has been evident from the increased threat activity they experienced on their network between May 2022 and October 2022 when compared to the six months prior. Not only are they seeing more activity – and not taking it seriously – but they're allowing the threat of cyberwarfare to impact innovation, admitting to stalling or stopping digital transformation projects as a result. Clearly, these threats are not ones to shy away from, as they need to be addressed head-on in order to be defended against.

Earlier in the report, the respondents who already spend the most on cybersecurity indicated that 37% are very likely to increase investment soon, and 41% somewhat likely. More than 2 in 5 (42%) of the IT and security professionals surveyed foresee their organization investing in **vulnerability management** immediately, while almost 3 in 10 (28%) said within six months. Regarding investments in **asset management**, 37% of respondents indicated their companies would make investments immediately, and 30% said they would invest within six months.

Whether a network attack is a result of a nation-state actor or cybercriminals, the impacts to an organization's operations and reputation are the same. Moreover, remote desktop protocol, bring your own device networks, virtual private network vulnerabilities, and protocol misconfigurations are becoming the most common entry point for attackers. This has been exacerbated by the pandemic, and in 2021, ransomware attacks **nearly doubled**[25] globally.

Having the correct tools in place in addition to an incident response (IR) plan is only the first step. Testing that plan regularly can help you proactively identify weaknesses in your cybersecurity and shore up defenses to help protect the critical data of businesses and consumers alike. Not to mention, this can save organizations millions in data breach costs.

Armis recommends the following measures for all organizations:

- Regardless of the tools and techniques an organization chooses to put in place, many organizations will need assistance mitigating the effects of an attack through the execution of an incident response plan. It is often good practice for an organization to put a specialist incident response team on retainer to reduce the cost and increase the speed of the incident response.
- Once an attack has been detected, minimizing the impact is essential. Islanding or isolation continues to be the predominant strategy for most organizations. There are a variety of isolation techniques, and most endpoint detection and response tools provide on-device isolation functionality. This allows incident responders the ability to isolate individual machines from the rest of the network.

- Furthermore, a good backup strategy and process is also a primary line of defense against both nation-state attacks and cybercriminals. Organizations should ensure that their chosen solution is resistant to attacks and should include continuous monitoring and integrity checking.
- A cyber-resilient organization will also invest in security awareness training for their employees. Ensure employees are regularly trained on how to identify malicious email traffic and provide easy-to-use reporting mechanisms.

Organizations should work under the principle that nation-state actors or cybercriminals will be successful in their efforts. After all, malicious actors only need to be successful one time out of all of their attempts to gain access to an organization's network, whereas security and IT teams need to be successful 100% of the time in their defense to prevent these attacks.

So, what can organizations do? Early detection and continuous monitoring is the best way to improve the 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.

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.**

REPORT DEMOGRAPHICS

To prepare this report, Armis commissioned a study with Censuswide, surveying 6,021 IT and security professionals in firms with more than one hundred employees across the USA, UK, Spain, Portugal, France, Italy, Germany, Austria, Switzerland, Australia, Singapore, Japan, the Netherlands, and Denmark. Responses were gathered between September 22, 2022 and October 5, 2022.

RESPONDENTS BY COUNTRY	
Australia	511
Austria	100
Denmark	50
France	501
Germany	501
Italy	500
Japan	501
Netherlands	52
Portugal	251
Singapore	501
Spain	500
Switzerland	50
UK	1003
USA	1000

RESPONDENTS BY TITLE/ROLE	
Chief Information Officer (CIO)	432
Chief Information Security Officer (CISO)	241
Chief technology officer (CTO)	530
Computer support specialist	229
Database administrator	457
Information security analyst	392
Information technology (IT) project manager	1831
Network administrator	394
Network architect	260
Other	346
Systems analyst	493
Web developer	416

RESPONDENTS BY VERTICAL	
Government, Local Authority, Public Sector Agency	369
Financial Services and Insurance	120
Healthcare, Medical, Pharmaceutical	255
OT (automotive, distribution, logistics and transport, food and beverage, manufacturing, oil, gas, construction, mining, agriculture, transportation)	1415
Technology and Other	3133
Retail and Wholesale	295
Telecommunications	434

ENDNOTES

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.ibm.com/reports/data-breach
9. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
10. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
11. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
12. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
13. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
14. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
15. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
16. https://www.ibm.com/reports/data-breach
17. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
18. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
19. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
20. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
21. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
22. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
23. http://stopransomware.gov
24. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
25. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

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®