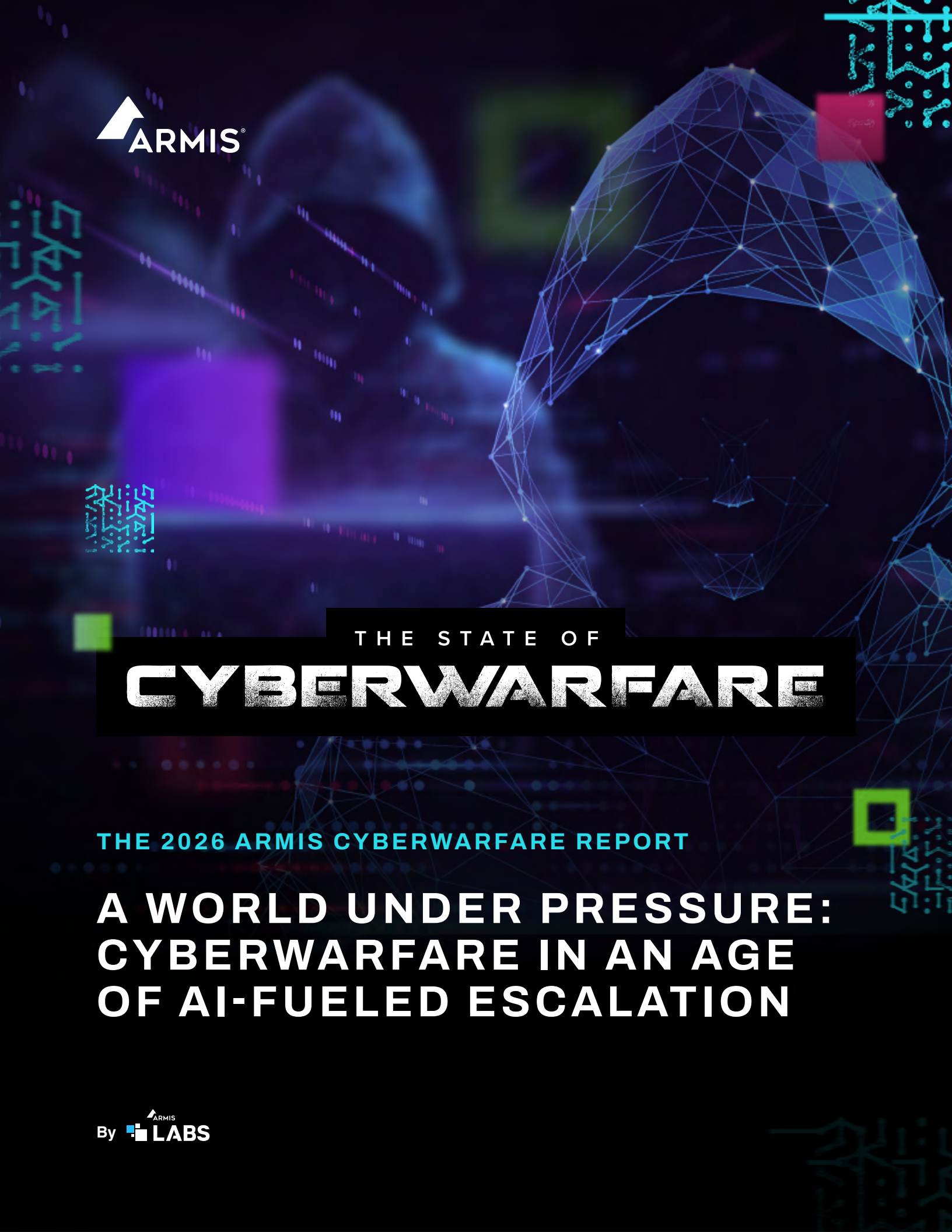


ARMIS®

THE STATE OF

CYBERWARFARE

THE 2026 ARMIS CYBERWARFARE REPORT

A WORLD UNDER PRESSURE: CYBERWARFARE IN AN AGE OF AI-FUELED ESCALATION

By ARMIS LABS

FOREWORD

By Nadir Izrael,
CTO and Co-Founder, Armis

In the four years since we launched our first State of Cyberwarfare report, the global threat landscape has shifted from a state of quiet concern to a total pressure cooker. What began in 2023 as a warning against organizational indifference has evolved at an exponential pace only paralleled by a rocket ship. We have moved with terrifying speed from the weaponization of history's largest election cycle in 2024 to the arrival of AI-supercharged warfare in 2025. Today, in 2026, we are no longer looking at a future threat; we are operating in a reality where the lines between digital disruption and physical conflict have effectively dissolved.

The acceleration we've witnessed over such a short period is a sobering reminder that our traditional timelines for defense are obsolete. We have entered a triple-threat era defined by fragmented geopolitics, the democratization of state-level destructive power via agentic AI, and a widening readiness gap. While awareness and fear of cyberwarfare have reached an all-time high and many industry-wide have made great strides to improve our readiness, our collective ability to defend is not yet keeping pace with the sheer velocity of our adversaries.

Today's organizations are in the crosshairs of autonomous, goal-seeking agentic AI. We're seeing cases of "agentic swarms" of AI agents that can autonomously discover vulnerabilities, write exploits, and move laterally across a network without human intervention. Telemetry suggests that the Mean Time to Compromise (MTTC) has dropped from hours to seconds when Agentic AI is deployed. In 2026, we could see 15% of observed 'Zero-Day' exploits discovered and weaponized by autonomous agents before human researchers can even categorize the CVE. We are facing a landscape of autonomous exploitation and systematic pre-positioning within our critical infrastructure that demands a move beyond reactive resilience.

However, this trajectory is not destiny. The data within this fourth annual report proves that while the threat has accelerated, so has our capacity for innovation. We are seeing a number of organizations worldwide successfully break the cycle of reactivity. By embracing AI-native, real-time exposure management, these leaders are proving that we can not only match the speed of our adversaries but outpace them. The "pressure cooker" of 2026 is creating a necessary diamond: a more resilient, proactive, and unified global defense.

The window to act is narrowing, but it remains open for those willing to shift their strategy. We have the tools, the intelligence, and the collective willpower to secure our future. By moving from a posture of fear to one of strategic, proactive action, we can turn the tide and ensure that our critical infrastructure and societal trust remain unshakeable. The call to action is clear, and the opportunity to lead the defense has never been greater. Let's meet this moment together.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The world is in geopolitical turmoil. Alliances are fracturing and Information and technology have become weapons of choice. In this environment, cyberwarfare has become a constant force destabilizing global relations, reshaping diplomacy, economic policy and strategic influence.

In the fourth edition of the Armis State of Cyberwarfare Report, this year's findings show cyber conflict entering a new phase. AI is now deeply embedded across economies, organizations, and everyday digital life. But with that dependency comes exposure. Today, 79% of IT decision-makers state that AI-powered attacks pose a significant threat to their organization's security, yet two thirds (66%) believe organizations underestimate the resources required to defend against those AI-powered threats. This rises to 75% in the United States.

Geopolitics is accelerating that gap. Rising tensions between the U.S., China, Europe, Russia, the Middle East and Latin America are playing out in what many now describe as an 'age of competition'. As geopolitical pressure builds, cyberwarfare becomes an increasingly attractive tool – fast, deniable, and scalable. AI simply sharpens that edge, and bad actors are already exploiting it. Two-thirds of organizations (66%) report experiencing up to two cybersecurity breaches, a four-percent increase from last year. As AI accelerates discovery, exploitation and lateral movement, the attack surface continues to expand, making cyberwarfare harder to detect, harder to contain and harder to recover from.

Against this backdrop, Armis revisits its annual State of Cyberwarfare findings to examine how attacks, methodologies and sentiment have evolved. This year's report surveyed more than 1,900+ IT decision-makers in companies with 1,000+ employees across the globe (see methodology for more details) to provide the latest comprehensive view of the growing threat landscape.

Armis Labs Insights

"In previous years, nation-states used proxy criminal groups to maintain distance," said Michael Freeman, Head of Threat Intelligence at Armis. "In 2026, our findings highlight a hybrid threat model where state actors use Agentic AI to automate the "noisy" parts of a breach (discovery and scanning), while humans "stay low" for the final objective."

> **The Technical Shift:** Attacks are no longer "events"; they are "states of being." Adversaries are pre-positioning within critical infrastructure, sometimes for months, using AI to map dependencies between IT and Operational Technology (OT).

> **The Risk:** If an AI agent autonomously triggers a kinetic effect, like a power surge, based on a hallucinated goal, the line between "cybercrime" and "act of war" evaporates instantly.

BACK TO TOP

KEY FINDINGS

Results at a Glance

78%

of IT decision-makers worldwide say geopolitical tensions globally have created a greater threat of cyberwarfare

68% believe the weaponization of AI will make cyber conflict a more persistent feature of global geopolitics

50% of global organizations were previously hacked, with IT leaders admitting they've still not managed to secure their ecosystem adequately

79% **of organizations are concerned about the potential for nation-state actors to use AI to develop more sophisticated and targeted cyberattacks**

69% Global reliance on AI will intensify the geopolitical stakes of cybersecurity, say 69% of IT pros

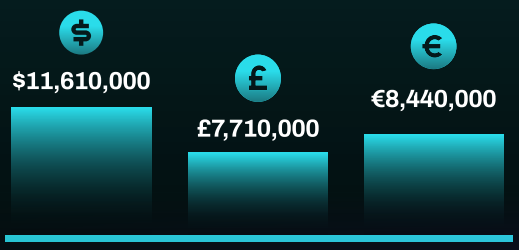
64% of IT leaders say emerging technologies will make it harder to distinguish between espionage, cybercrime, and acts of war

67% of IT professionals worldwide believe **the misuse of emerging technologies will increase the likelihood of collateral damage to civilian infrastructure in times of cyber conflict**

52%

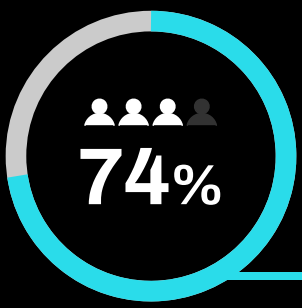
of respondents say their organization's average ransomware payout exceeds its annual cybersecurity budget

Average global ransomware payout in 2025:



Armis Labs Insights

In addition to a payout amount, there are recovery costs to consider. Often, business interruption and data restoration costs are 3X a ransom demand. Armis is a strong advocate of immutable backups and zoning.



of organizations have evolved their cyberwarfare readiness posture over the past 3 years to strengthen their defenses against nation-states

BACK TO TOP

01 DESTABILIZING TRUST ACROSS THE GLOBAL LANDSCAPE

More than three-quarters of IT decision-makers (78%) say geopolitical tensions have created a greater threat of cyberwarfare, a rising figure when compared to last year. Confidence in restraint is eroding too. Nearly three in ten (29%) no longer believe "Mutually Assured Disruption", where nations avoid major cyberattacks due to shared vulnerability, acts as an effective deterrent.

This erosion is unfolding alongside widening geopolitical rifts. What began with global tariffs and export controls being used as tools of coercion and competition, has hardened into a far more volatile international landscape. Instability in the Middle East has become just another flashpoint in a year marked by more abrasive politics, while Russia's continued aggression against Ukraine has pushed NATO closer to the frontline of deterrence.

All of this is unfolding while cyber conflict rages, destabilizing rivals without triggering open warfare. Except now, trust itself is the target. In fact, 74% of respondents agree that cyberwarfare attacks will increasingly focus on institutions representing free press and independent thinking, rising to 83% in Australia. AI-generated content, deepfakes and coordinated disinformation campaigns are already distorting narratives around real-world events. Manipulated media spreads at speed, eroding confidence and certainty while inciting fear, anger and paranoia.

Armis Labs Insights

In 2026, disinformation can evolve into cognitive warfare. Using leaked Personally Identifiable Information (PII) and AI to target specific high-value individuals, like CEOs or government officials, with deep-trust social engineering. We are now moving from mass disinformation to micro-targeted psychological exploitation.

In 2026, we predict a 300% increase in 'CEO-Clone' voice and video attacks. Cyber threat intelligence data shows that 1 in 4 mid-level managers fell for an AI-generated video request from their supposed 'executive' because the AI utilized stolen personal data (e.g. social media habits or speech patterns) to build a 'Deep Trust' profile."

When asked who they believe is driving this threat, respondents point to familiar geopolitical fault lines. Russia (62%) and China (55%) dominate perceptions of cyber risk, followed by North Korea (37%) and Iran (19%), reinforcing how the erosion of trust is being shaped by the global power competition (Fig. 1).

BACK TO TOP

Armis Labs Insights

It's essential that security teams do not introduce potential blind spots while playing the difficult attribution game. By over-focusing on the who, teams can potentially ignore the how. For example, a team cannot focus purely on defending against China, as they might miss a localized criminal group using the same Tactics, Techniques and Procedures (TTPs). Organizational defenses must be threat-agnostic.

Fig 1.

Fig 1. From which countries do you believe threat actors pose the most cybersecurity risk (to society, your home country, your industry, etc.)

Despite this, a contradiction persists. While four out of every five IT decision-makers (80%) say their organization is taking steps to address AI-generated disinformation and propaganda campaigns, over half (54%) admit they lack the budget and resources needed to invest in AI-powered security solutions, up from 49% last year.

This imbalance matters, because the pressure is not easing; combating AI-driven threats requires AI-driven defenses and 68% of respondents believe the weaponization of AI will only make cyber conflict a more persistent feature of global geopolitics. As tensions fray, AI-powered cyberwarfare is becoming harder to contain, harder to deter and harder to defend against. Without the proper countermeasures and technology in place, AI-driven attacks become impossible to deter or recover from which raises the critical question: **are organizations actually ready for this new world order?**

02 THE READINESS PARADOX WIDENS

On the surface, confidence remains high. Nearly eight in ten organizations (79%) say they're prepared to handle a cyberwarfare attack, and 76% believe they're ready to mitigate an AI-driven cyber threat. Awareness is no longer the issue. And 80% of IT decision-makers are confident in their organization's ability to detect and respond to a coordinated cyberattack.

But that confidence doesn't translate into resilience. More than half (54%) of organizations report being impacted by an AI-generated or AI-led attack in the past 12 months, while 66% say their organization has experienced up to two cybersecurity breaches, up from the year before. More concerning still, half of organizations (50%) admit they've been unable to adequately secure their ecosystems following an attack, rising to 57% for those working for a U.S. Federal government agency. Preparedness, it seems, is not keeping pace with threat evolution.

Nowhere is the paradox clearer than in how organizations are approaching AI itself. As AI becomes the top investment priority, 82% of IT decision-makers now say they've implemented measures to detect and counter AI-powered attacks. Additionally, 78% report they've increased investment into AI-enhanced security tools over the last year than in previous years.

Yet ambition continues to outpace capability. More than half (55%) of global IT decision-makers admit they still lack the necessary expertise needed to implement and manage these AI-powered security solutions effectively, a five-point increase year-on-year. For those IT leaders working in critical infrastructure, specifically Oil, Gas, Mining, Construction, and Agriculture organizations, that lack of expertise skyrockets to 78%. These gaps in skills and operational maturity risk becoming force multipliers for attackers rather than safeguards.

Armis Labs Insights

Compliance success is often mistaken for technical resilience. Organizations may feel ready because they pass audits, not because they can stop an autonomous agent. The security leaders surveyed may over-report satisfactory structures to avoid the appearance of professional negligence. Additionally, they may be underestimating simple tasks, like patching, while overestimating their capability on complex ones, including AI nation-state defense.

Strategic action plan for security leaders to better understand their declared vs. demonstrated readiness:

> **1. Shift Metrics:** Move from subjective sentiment to objective Mean Time to Detection (MTTD) validation.

> **2. Continuous Validation:** Replace static annual surveys with real-time Breach and Attack Simulation (BAS).

> **3. Red Team the AI:** Specifically pressure-test AI defenses to see if they hold up against machine-speed evasion techniques.

Detection challenges further expose the gap (Fig. 2), with a significant proportion (43%) of organizations still detecting and responding to a significant attack reactively; only as it occurs (27%) or after the damage has already been done (16%).

Fig 2

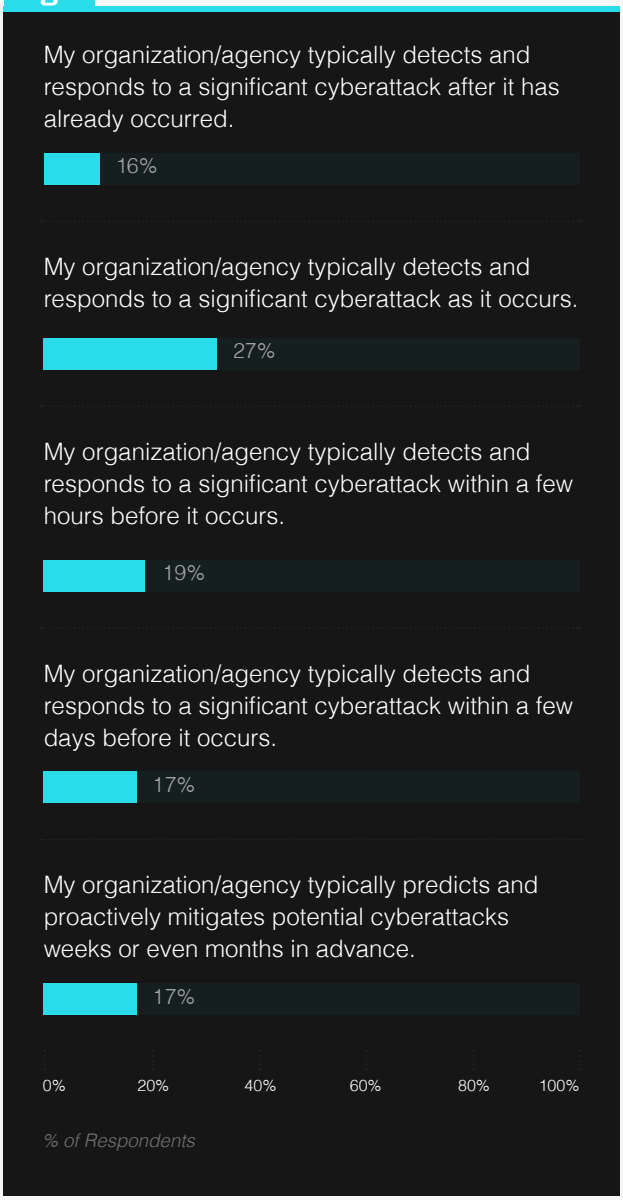


Fig 2. Response times of organizations.

Reacting late is increasingly indistinguishable from being unprepared. Organizations are finding themselves stretched between expanding attack surfaces, rising expectations and operational reality. This readiness gap carries a growing price tag in more ways than one.

BACK TO TOP

Armis Labs Insights

Shadow AI is another phenomenon important to callout as part of this year's report, as there's been a rise in employees using unauthorized AI tools that leak corporate IP into public Large Language Models (LLMs). As a result, we believe 2026 will be the year of the AI Leak.

71% of employees admit to using unvetted AI productivity agents. As a result, we estimate that 15% of proprietary corporate codebases have been leaked into public training sets, allowing adversaries to use those same AI tools to find backdoors in commercial software via simple prompting.

03 THE COST OF CYBERWARFARE WORSENS

As cyberwarfare becomes more persistent and harder to contain, the consequences are no longer limited to disruption alone. The financial, operational and strategic costs are escalating, with more than half of organizations (52%) now saying their average ransomware payout exceeds their annual cybersecurity budget.

In other words, reacting to a single incident can wipe out a year of planned security investment. What makes this more striking is how ransomware is perceived relative to other threats. Despite its outsized financial impact, ransomware only ranks fourth among the cybersecurity threats IT decision-makers say concern them most. The disconnect reflects a reality many organizations now face; ransomware is a powerful financial weapon, but it competes for attention with a growing set of equally damaging risks, stretching budgets and resilience across the board.

Avoiding payment is also becoming increasingly difficult. The proportion of organizations able to say "we have not had to make a ransomware payout" has fallen sharply year-on-year, signaling that payment is becoming the norm rather than the exception. The shift is most noticeable in key markets: in the U.S., this figure drops from 40% to 30% year-on-year, while in Australia, it's fallen from 44% to 25%. More organizations are simply being forced to pay.

For those that do, the costs are significant. According to the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), ransomware payments surpassed more than $4.5 billion in total reported payments over the past decade, underscoring the sustained economic toll of cyber extortion. At the same time, the average payout of a single ransomware attack continues to climb across regions (Fig. 3).

Fig 3

Fig 3. Average cost of a ransomware payment (regional).

These figures reflect a broader shift in attacker behavior. Ransomware is no longer deployed in isolation, but as part of multi-stage campaigns designed to maximize disruption and payout. Organizations report a wide range of offensive techniques regularly bypassing security tools (Fig. 4), from phishing to the exploitation of misconfigured cloud environments.

BACK TO TOP

Fig 4

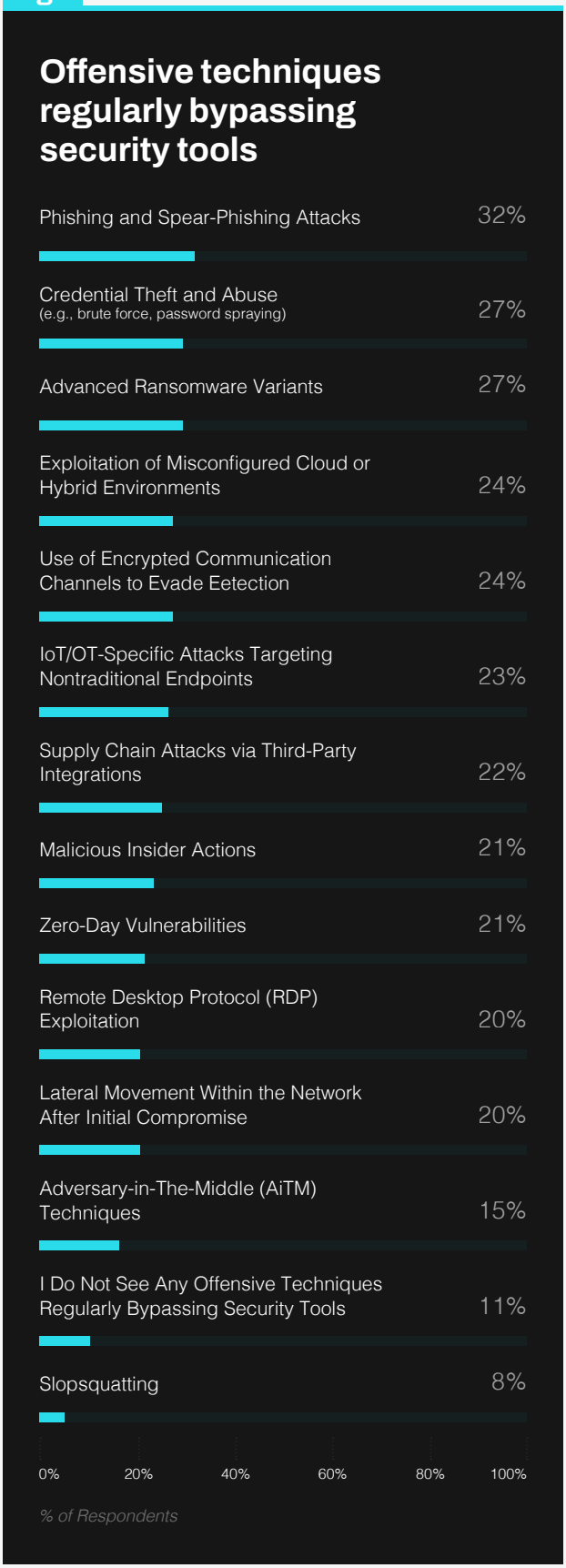


Fig. 4. Offensive techniques regularly bypassing security tools

This is unfolding despite growing regulatory pressure. In the U.S., states such as New York have moved to ban ransom payments by public-sector bodies, while federal agencies continue to push for faster incident reporting and greater transparency. Elsewhere, governments are taking similar steps: the UK has also proposed banning ransom payments across public bodies, while Australia has become the first country to force disclosure of ransomware payments within 72 hours.

Yet regulation is struggling to keep pace. In fact, 65% of IT decision-makers agree the current pace of AI innovation is outrunning cybersecurity policy and regulation. Attackers are moving faster, blending financial extortion with operational disruption. Cyberwarfare is now a material business risk and the pace of change shows no sign of slowing.

Armis Labs Insights

In 2026, ransomware has matured into a professionalized business model focused on Quadruple Extortion.

1. **Encryption -** Locking your data.
2. **Exfiltration -** Threatening to leak sensitive info.
3. **DDoS -** Hammering your customer-facing portals during negotiations.
4. **Supply Chain Pressure -** Contacting your customers and suppliers directly to inform them that their data was stolen from your network, effectively weaponizing your business relationships against you.

It is essential that security teams be aware of the evolving threat landscape to effectively protect their organization from impact.

04 WHO HAS IT WORSE?

By Industry

Financial Services, Insurance

- 84% of IT decision makers working within the sector agree with the statement, “My organization is concerned about the potential for nation-state actors to use AI to develop more sophisticated and targeted cyberattacks.” This is up from 72% last year.
- 64% of respondents agree that the current pace of AI innovation is outrunning cybersecurity policy and regulation.
- 64% of financial services and insurance organizations have experienced 1-2 breaches, an increase on 58% from last year.

Manufacturing, Engineering

- 79% of IT decision-makers working with the sector say the cyber capabilities of nation-state actors have the potential to instigate full-scale cyberwar that could cripple critical infrastructure worldwide, rising 6 points from the year prior.
- 65% of manufacturing and engineering organizations have experienced 1-2 breaches, a rise from 60% in our 2025 report.
- 42% of respondents said they regularly see phishing and spear-phishing attacks bypassing security tools – a jump from the 30% figure last year.

Government, Local Authority, Public Sector Agency

- 81% of IT decision makers working within the sector believe that geopolitical tensions globally have created a greater threat of cyberwarfare.
- 53% of respondents agree their organization lacks the necessary budget and resources to invest in AI-powered security solutions, an increase from 48% in last year’s findings.
- 31% ranked, “having insufficient budget to fully scale cybersecurity operations,” as their biggest security gap.

Medical, Healthcare, Pharmaceutical

- Over half (53%) of IT decision makers say that the threat is imminent and have had to report an act of cyberwarfare to the authorities – a massive jump from the 37% who shared the same last year.
- 64% of respondents working within the sector agree that most organizations are unprepared for the scale of investment required to keep pace with AI-enabled adversaries.
- 58% also agree their organization lacks the necessary budget and resources to invest in AI-powered security solutions, a rise from 50% last year.

BACK TO TOP

Oil, Gas, Mining, Construction, Agriculture

- 68% have also experienced more threat activity on their network in the past six months than the six months prior – a rise in 31% from the year prior.
- 76% of IT decision makers working within the sector say their organization's average ransomware payout exceeds its annual cybersecurity budget.
- 41% of respondents highlighted that when making a ransomware payout, their organization pays between $10M - $30M, a significant increase on the 16% of respondents from this sector who answered the same in our prior report.

Technology

- To stay ahead of emerging AI-powered threats, 86% of IT decision-makers working within the sector say their organization has invested more in AI-driven security tools and solutions over the last year than in previous years.
- Yet, 58% agree that their organization lacks the necessary expertise to implement and manage AI-powered security solutions effectively.
- 67% of respondents agree that increased M&A activity among technology companies has further complicated the cybersecurity programs of organizations.

Retail/Wholesale Services

- Two-thirds (74%) of IT decision makers working within the retail sector say cyberwarfare threats are increasingly targeting unmanaged or supply chain assets not visible to traditional security tools.
- 70% of respondents say they're reconsidering suppliers and increasing cybersecurity investments as a result of geopolitical tensions and increased cyber risk.
- A quarter (24%) of IT decision makers highlighted their biggest security gap is a difficulty in identifying and managing shadow IT or ephemeral assets.

BACK TO TOP

KEY REGIONAL FINDINGS

UNITED STATES

92% Over 9 in 10 (92%) IT decision makers in the U.S. are concerned about the impact of cyberwarfare on their organization as a whole.

83% U.S. respondents (83%) were most likely to agree with the statement: "My organization has allocated sufficient budget for cybersecurity programs, including people and processes." Yet, 61% say their organization's average ransomware payout exceeds its annual cybersecurity budget.

61% 61% of respondents from the U.S. – the most of respondents from any country surveyed for this report – said their organization was previously hacked and they've not yet managed to secure their ecosystem adequately.

UNITED STATES
FEDERAL

81% 81% of respondents working for the U.S. Federal government believe their agency is prepared to handle a cyberwarfare attack and respond to related threats.

57% Yet over half (57%) say their agency was hacked previously and they've not managed to secure their ecosystem adequately.

77% 77% agree the misuse of emerging technologies will increase the likelihood of collateral damage to civilian infrastructure in times of cyber conflict.

UNITED KINGDOM

81% 81% of respondents from the UK are confident in their organizations' ability to detect and respond to coordinated cyberattacks.

66% Yet, 66% have experienced 1-2 cybersecurity breaches, with 39% saying their organization has not yet managed to secure their ecosystem adequately following these attacks.

54% Additionally, IT decison makers in the UK (54%) are the second most likely of respondents from any country to say the cyberwarfare threat is imminent, sharing they have already had to report an act of cyberwarfare to authorities.

BACK TO TOP

FRANCE

80% | 80% of respondents from France think geopolitical tensions globally have created a greater threat of cyberwarfare.

40% | 40% of French respondents say they experienced more threat activity in the second half of 2025 when compared to the first half of the year. Another 45% say they've experienced a consistent level of threat activity.

41% | 41% of French organizations respond reactively to a significant cyberattack, either as it occurs (24%) or after it as already occurred (17%).

GERMANY

57% | Respondents from Germany (57%) are least likely to believe that nation-states would target their organization.

68% | 68% of respondents say their organization is prepared to handle a cyberwarfare attack and respond to related threats. However, 44% of German businesses that were hacked previously have still not managed to secure their ecosystem adequately.

46% | 46% of IT professionals in Germany said "no" when asked if their own government can defend its citizens and enterprises against an act of cyberwarfare.

ITALY

78% | 78% of Italian IT decision makers are concerned about the impact of cyberwarfare on their organization as a whole.

54% | 54% of IT professionals say the complex regulatory ecosystem has overwhelmed their security team.

38% | Only 38% of respondents from Italy are confident that their government can defend its citizens and enteprises against an act of cyberwarfare.

BACK TO TOP

EUROPE

86% 86% of IT decision makers in Europe are concerned about the impact of cyberwarfare on their organization as a whole.

43% 43% of respondents across Europe say that the cyberwarfare threat is imminent and that they have had to report an act of cyberwarfare to authorities.

71% 71% of European IT professionals believe the cyber capabilities of nation-state actors have the potential to instigate a full-scale cyberwar that could cripple critical infrastructure worldwide.

AUSTRALIA

95% 95% of IT decision makers in Australia are concerned about the impact of cyberwarfare on their organization as a whole, the most of any country surveyed.

72% Respondents from Australia (72%) are the most likely to say the cyberwarfare threat is imminent; sharing they have already had to report an act of cyberwarfare to authorities.

84% Australian respondents (84%) were the most likely to say their organization has evolved its cyberwarfare readiness posture over the past three years to strengthen defenses against nation-states.

BACK TO TOP

05 EMERGING TECHNOLOGIES AND THE NEXT PHASE OF ESCALATION

This year's findings show cyberwarfare entering a new phase, defined by speed, scale and autonomy. Nearly two-thirds of organizations (65%) report having already experienced an application-based attack, while 69% agree that AI will enable non-state actors to operate with nation-state-level sophistication. The barriers to entry are gone, even as the impact of attacks continues to rise.

Nearly eight in ten IT decision makers (79%) are now concerned that nation-states will use AI to develop more sophisticated and targeted cyberattacks, up from 73% the year prior. Yet confidence in the foundations of modern software development remains high, reinforcing the readiness paradox. For example, more than three-quarters (77%) trust the integrity of third-party code libraries, and the same proportion believe AI-generated or AI-assisted code is thoroughly checked for high-severity vulnerabilities.

Armis Labs Insights

In 2026, we're seeing increased risk as a result of AI-generated Vibe Coding. Developers are increasingly using LLMs to ship code at record speeds, often focusing on the "vibe" (it works) rather than the "security" (it's robust).

> **The Exposure:** 77% of leaders trust third-party code libraries, yet AI-generated modules are introducing silent vulnerabilities that traditional scanners miss because the code is syntactically correct but logically flawed.

> **The Fallout:** We are seeing the first cases of AI-poisoned supply chains, where malicious code is subtly injected into open-source dependencies by adversarial AI agents, which then spread downstream to thousands of enterprises.

That confidence sits uneasily with reality. Concerns remain high around reliability, from hallucinations in large language models to automation errors that are difficult to detect at scale, particularly as code is generated by AI, deployed and iterated at machine speed. Even major cloud service providers have faced recent near misses as a result of a code vulnerability that could've caused supply chain chaos and risked thousands of users.

The risks don't stop with AI. Sixty-nine percent of IT decision makers believe a large-scale quantum computing attack could render their most sensitive encrypted data readable by a hostile state actor within the next decade. A quarter (24%) already fear quantum computing to be the greatest future existential risk if weaponized (Fig. 5). But waiting for these capabilities to fully mature before acting is a dangerous assumption.

Fig 5

Fig. 5. Which emerging technology, if weaponized, poses the greatest future existential risk to your organization's/agency's security?

BACK TO TOP

Geopolitical competition is accelerating this shift. Nations are scrambling to secure the computing power, talent and infrastructure needed to dominate emerging technologies. China claims it's already testing over ten experimental quantum-based cyber weapons designed specifically for warfare, while Russia is building quantum navigation to counter electronic warfare too. These advancements are compressing years of capability development into a much shorter window, threatening to reshape cyber conflict faster than defensive models can adapt.

Armis Labs Insights

When considering emerging technologies and the next phase of escalation, it's critical to also consider space-terrestrial convergence, or the orbital attack surface. This has triggered increasing concern from all nations with space-based capabilities.

In 2026, cyberwarfare is no longer earthbound. The proliferation of Low Earth Orbit (LEO) satellite constellations for global internet and military communications represents a critical blind spot. As such, conflict in 2026 now involves the systematic targeting of ground-to-space links.

Attacks on satellite ground stations are predicted to increase by 115%. 62% of critical infrastructure organizations now rely on space-based assets for Positioning, Navigation, And Timing (PNT) services, yet only 12% have specific security protocols for satellite-linked technologies.

And yet, many defensive responses remain foundational (Fig. 6). Measures such as multi-factor authentication and password policies are still widely relied upon. While necessary, they're no longer sufficient on their own in the face of autonomous, machine-speed threats. This is further hampered by operational gaps.

Fig 6

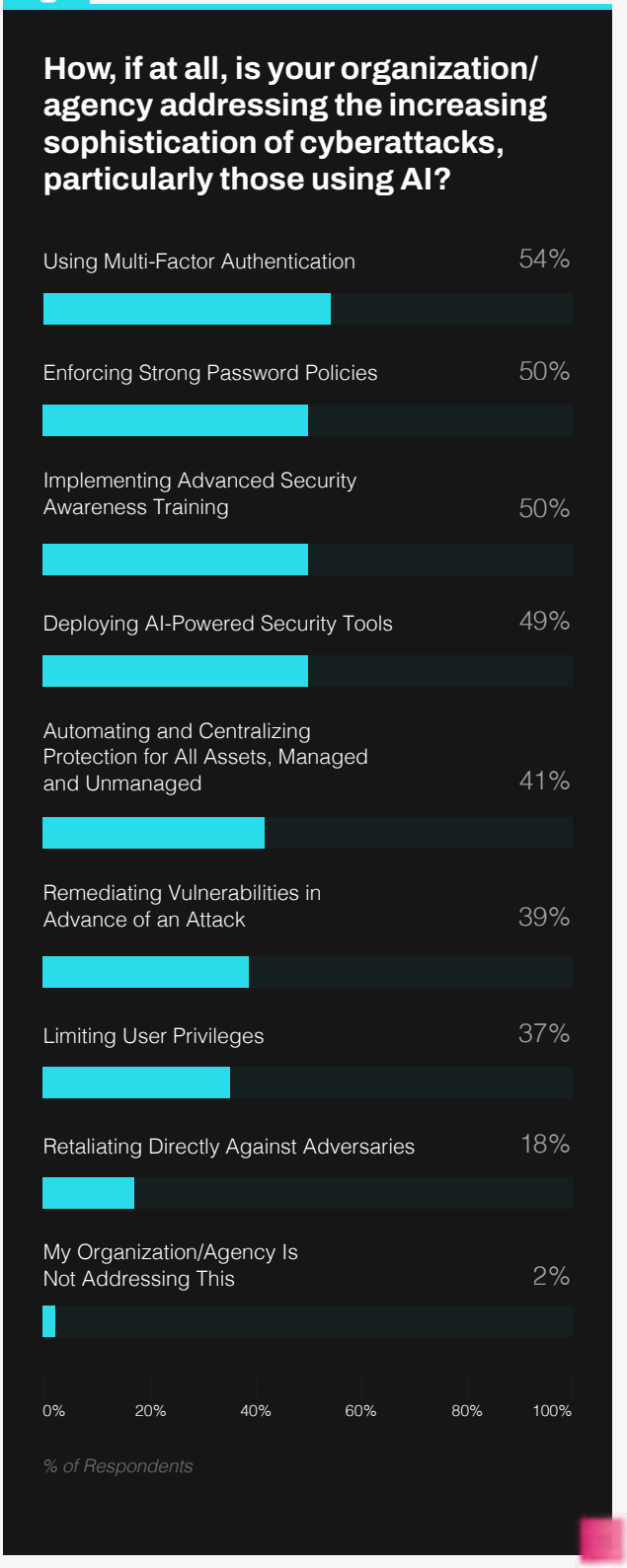


Fig. 6. How, if at all, is your organization/agency addressing the increasing sophistication of cyberattacks, particularly those using AI?

A year-on-year comparison shows many challenges have not been resolved, only normalized (Fig. 7). Issues such as cloud security limitations, threat prioritization and alert overload continue to affect around one in five organizations. More strikingly, one in ten (13%) of organizations still believe they have no security operational gaps at all, a level of confidence that sits uneasily alongside the scale and complexity of emerging threats.

Fig 7

What gaps do your security operations have, if any?

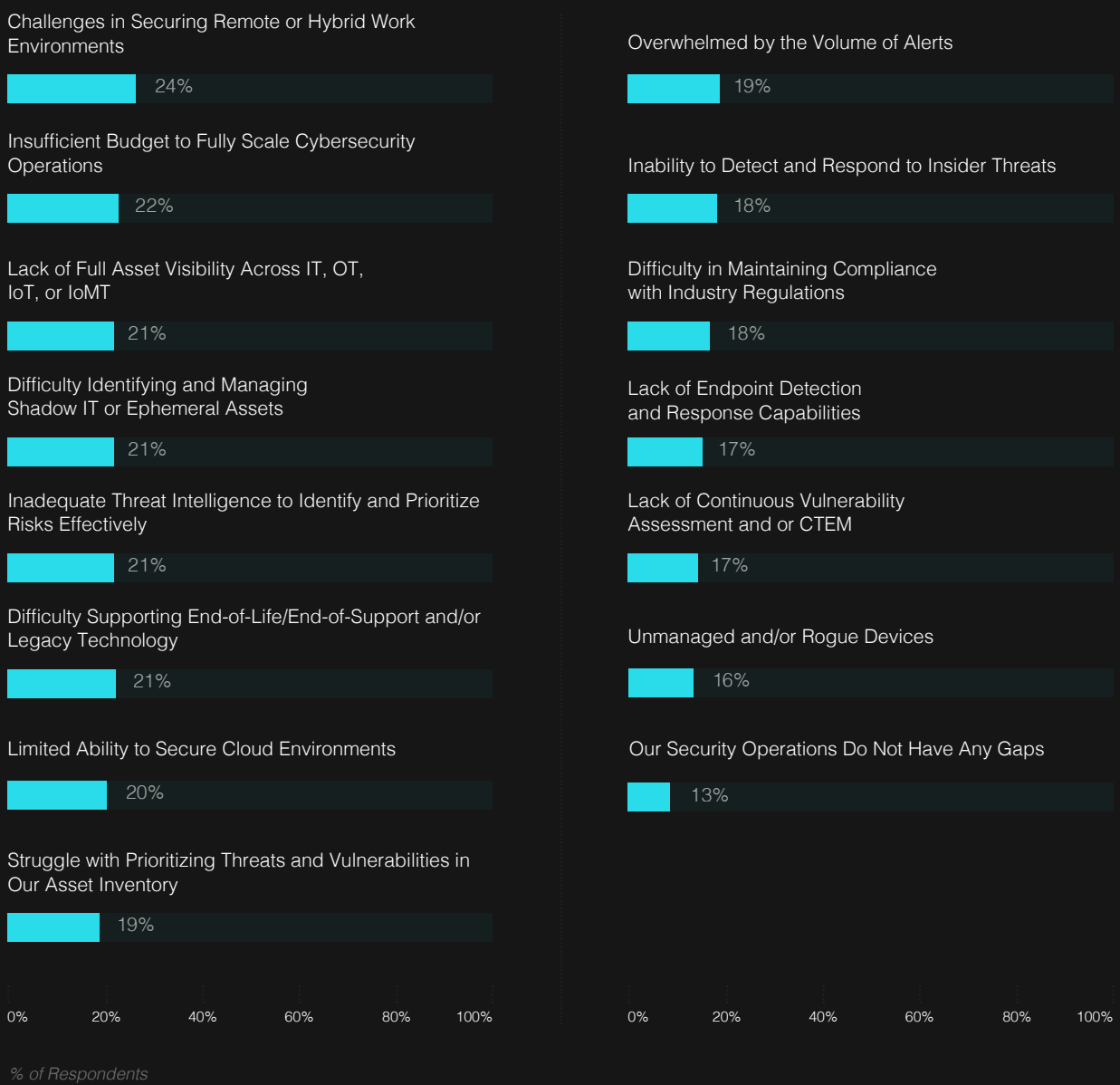


Fig. 7. What gaps do your security operations have, if any?

BACK TO TOP

It's this convergence – AI, quantum and other emerging technologies – that defines the next phase of escalation. That's why 65% of IT decision makers agree that this convergence will drive an unprecedented escalation in cyber conflict capabilities, while 67% believe this misuse will increase the likelihood of collateral damage to civilian infrastructure. It's a dangerous world and it's simply the result of years of mounting pressure, technological acceleration and trust being eroded.

06 ANALYZING THE COMPRESSED EVOLUTION OF CYBERWARFARE

When Armis published its first State of Cyberwarfare report in 2023, cyber conflict was still unevenly understood. One third of organizations (33%) was not taking the threat of cyberwarfare seriously, identifying as indifferent or unconcerned about the impact of cyberwarfare, leaving room for blind spots and unaddressed risk.

By 2024, awareness had not translated into clarity. Almost half (46%) of IT leaders said they were unconcerned or indifferent about the impact of cyberwarfare. Not because the threat had diminished, but because organizations were grappling with an overwhelming volume of data, alerts and competing risks. At the same time, cyberwarfare was becoming impossible to ignore. Thirty-nine percent of IT leaders believed cyberwarfare could undermine the integrity of elections, and 42% warned it could be used to target the media, in a year when more than 70 countries went to the polls.

In 2025, the shift accelerated. As AI began to fundamentally reshape the threat landscape, nearly three-quarters (73%) of IT decision-makers globally expressed concern about nation-state actors using AI to develop more sophisticated and targeted cyberattacks. Perception flipped decisively: 87% said they were finally concerned about the impact of cyberwarfare on their organization, while indifference collapsed to just 11%. AI compressed years of evolution into months.

This year's data shows where that trajectory has led. Concern has risen again to 89% of IT decision-makers, with 48% now describing themselves as very concerned. As trust between nations frays, 78% agree that geopolitical tensions globally have created a greater threat of cyberwarfare.

What began as a misunderstood risk has become an always-on condition shaped by geopolitics, technology and systemic dependency. AI did not create cyberwarfare, but it removed the pauses. And in a world defined by constant tension, speed and uncertainty, that reality is likely to worsen, unless action is taken.

BACK TO TOP

RESILIENCE IN AN ERA OF AI-ACCELERATED CYBERWARFARE

The findings in this report point to a clear reality: cyberwarfare is constant, accelerated by technological evolution and shaped by global competition. The pace of change is not slowing. What organizations understand about their risk today may be fundamentally outdated within a year. In this environment, organizations need to better understand their exposure – continuously, in context and at scale.

Cyber exposure management becomes essential. The advantage belongs to those who can see their entire environment, understand how assets connect and change, and act before attackers exploit the gaps. Exposure management shifts security away from chasing individual alerts and towards addressing root causes, revealing which assets matter most, where trust is misplaced and how small weaknesses can cascade into systemic risk.

Armis delivers this capability through Armis Centrix™, the leading AI-powered Cyber Exposure Management Platform. Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects the entire attack surface of organizations before there's any impact to a business' environment.

AI plays a critical role in this shift, but only when applied with context. Armis uses AI to correlate behavior, vulnerabilities and dependencies across complex environments, transforming fragmented signals into actionable insight. This allows security teams to focus on the exposures that matter most – prioritizing real-world risk over noise.

In a world where cyberwarfare is constant and geopolitical escalation is the norm; resilience is no longer defined by response alone. It's defined by anticipation. Cyber exposure management gives organizations the ability to adapt as the landscape shifts, maintaining awareness as new technologies, assets and dependencies emerge, and acting decisively before exposure becomes impact.

BACK TO TOP

ARMIS CENTRIX™

DISCOVER NEW APPROACHES TO PROTECTING YOUR ORGANIZATION

Armis Centrix™ acts as air traffic control for your entire digital estate. It delivers real-time visibility into every managed, unmanaged, and IoT device, **no agents required.** By leveraging the world's largest Asset Intelligence Engine, it clears the fog of shadow assets to prioritize and neutralize risks before they're ever weaponized.

Experience Armis Centrix™

BACK TO TOP

METHODOLOGY

The research was conducted by Censuswide, among a sample of 1,905 IT decision-makers at companies with 1,000+ employees across the UK, US, Australia, France, Germany, and Italy. 'Europe' refers to data from the UK, France, Italy and Germany grouped.

The data was collected between 24.11.2025 – 08.12.2025

Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

BACK TO TOP

ARMIS®

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com