auxis
A Grant Thornton US company

10 Cybersecurity Trends Redefining the Future of Defense

From AI-powered threats to new operating models, discover how leading organizations are reshaping cyber strategy in 2026

The Cybersecurity Reset: What Security Leaders Need to Know in 2026

Cybersecurity has, in the space of a few years, evolved from a back-office IT task into a boardroom imperative. For four consecutive years, it's held the top spot on the 2025 Allianz Risk Barometer[1] as the No. 1 concern for businesses worldwide.

Today, cybersecurity is a core business priority, with CIOs, CISOs, and a growing number of new C-level leaders driving strategies to protect critical infrastructure, safeguard data, and ensure business continuity.

So, what's changed? AI, for one. Rapid advances in artificial intelligence have ushered in powerful new capabilities such as Generative AI (GenAI) and Agentic AI – fundamentally reshaping the cybersecurity battlefield. With GenAI tools now freely available and widely adopted, malicious actors can launch more frequent, sophisticated, and targeted cyberattacks – exploiting new vulnerabilities and multiplying entry points across the digital landscape.

Attacks against organizations worldwide have ramped up significantly: Businesses now face an average of 1,673 attacks per week, a 44% jump from a year earlier! (Check Point's 2025 Cyber Security Report[2]).

In this landscape, it's no surprise 93% of board members now consider cyberthreats a direct risk to shareholder value (Gartner's 2025 Top 3 Strategic Priorities for Security and Risk Management Leaders research[3]). Worse, 98% believe cyberthreats will only grow over the next two years.

But while cybersecurity stands as a top investment area for CIOs, funding has not kept pace with the scale of the challenge.

Average security budgets grew just 4% year over year in 2025 (IANS 2025 Security Budget Benchmark Report[4]), even as the complexity of programs – and the cost of talent, tools, and training – continues to rise. In fact, the share of IT spend devoted to security is shrinking, as organizations divert funds to chase the growth and efficiency promised by AI and cloud initiatives.

In this climate, how can organizations improve their cybersecurity posture?

Understanding the forces reshaping the cybersecurity landscape – and learning how to prove the business value of proactive investments – are essential first steps. This report uncovers the top cybersecurity trends for 2026 – and offers practical guidance for aligning strategy, resources, and leadership to stay one step ahead of tomorrow's threats.

Jose Alvarez
Managing Director of IT Services
Auxis

Table of Contents

10 Cybersecurity Trends Reshaping 2026

1. Data Breach Costs Touch Record High in U.S.

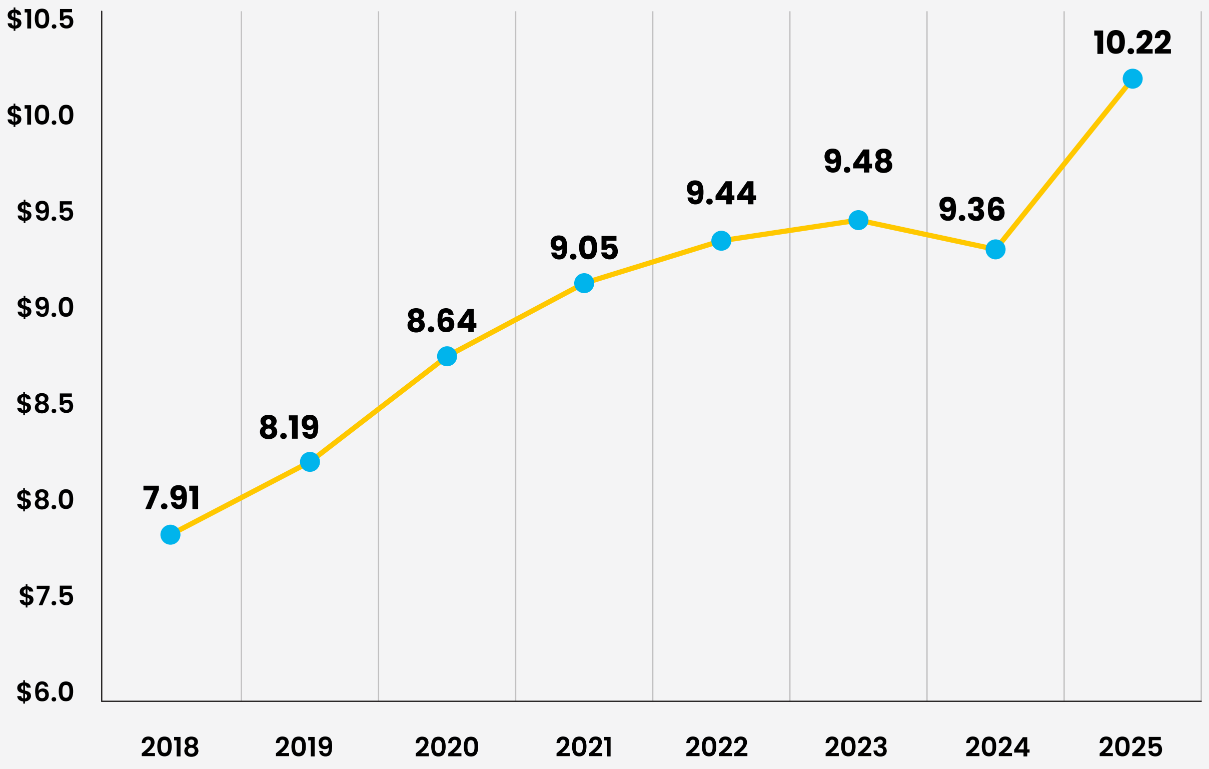
For five years, global data breach costs rose steadily, fueled by AI-powered attacks and too many organizations reactively investing in cybersecurity *after* a breach.

2025 brought the first glimmer of good news: Average global breach costs fell to $4.44 million, down from $4.88 million in 2024, as enterprises increasingly leveraged AI and automation to detect and contain threats faster, IBM's 2025 Cost of a Data Breach report[5] found.

Yet, the United States saw a different story: breach costs surged to $10.22 million, a 9% jump over the previous year and the highest worldwide.

Data Breach Costs in the U.S.

Measured in USD millions



Source: IBM's 2025 Cost of a Data Breach report

> **Breach costs in the United States surged to $10.22 million in 2025, a 9% jump over the previous year and the highest worldwide.**
>
> *IBM's 2025 Cost of a Data Breach report*

So, why is the U.S. still trending the wrong way?

Higher regulatory fines

The United States remains a sustained target for attackers. In Q2 2025, North America accounted for 53% of known ransomware attacks alone – the highest of any region, according to Check Point's latest quarterly security trends report[6].

This relentless wave of breaches – including major consumer data leaks in recent years at Yahoo, National Public Data, Facebook, and Target – has exposed massive amounts of consumer data and prompted regulators to respond with tougher frameworks and steeper penalties.

Regulatory fines in the U.S. are enforced by multiple state, federal, and industry bodies – meaning a patchwork of agencies can impose sanctions for the same incident. HIPAA violations alone can cost healthcare organizations over $2 million annually.

The result: U.S. organizations now face the world's highest post-breach regulatory costs, the IBM report found – underscoring the financial stakes of inadequate cybersecurity.

Increased detection and escalation costs

Globally, shorter breach investigations, aided by AI and automation, are pushing down detection and escalation costs. These costs include assessments and audits, crisis management, and communications to executive leadership and boards.

However, detecting cyberattacks in the U.S. is traditionally more challenging. Here's why:

- An abundance of complex, interconnected IT environments providing more entry points for attacks.
- The U.S. has a massive attack surface, with the largest number of connected devices, users, and organizations globally.
- More sophisticated and persistent threats due to the country's highly digital economy.
- Many organizations, especially small and midsize businesses, face steep cybersecurity talent shortages as well as lack of access to modern detection tools (e.g., SIEM, EDR, XDR).
- Fragmented security practices and regulations across industries and states.

As a result, detection tends to be slower – giving attackers more time to do damage and steal or compromise data, leading to higher costs. Many times, companies aren't even aware of a breach until after an attacker discloses it – giving the attacker ample time to wreak havoc.

> **When attackers – not internal teams – reveal a breach, the average global cost soars to $5.08 million, more than 20% higher than when organizations catch the breach ($4.18 million).**
>
> *IBM's 2025 Cost of a Data Breach report*

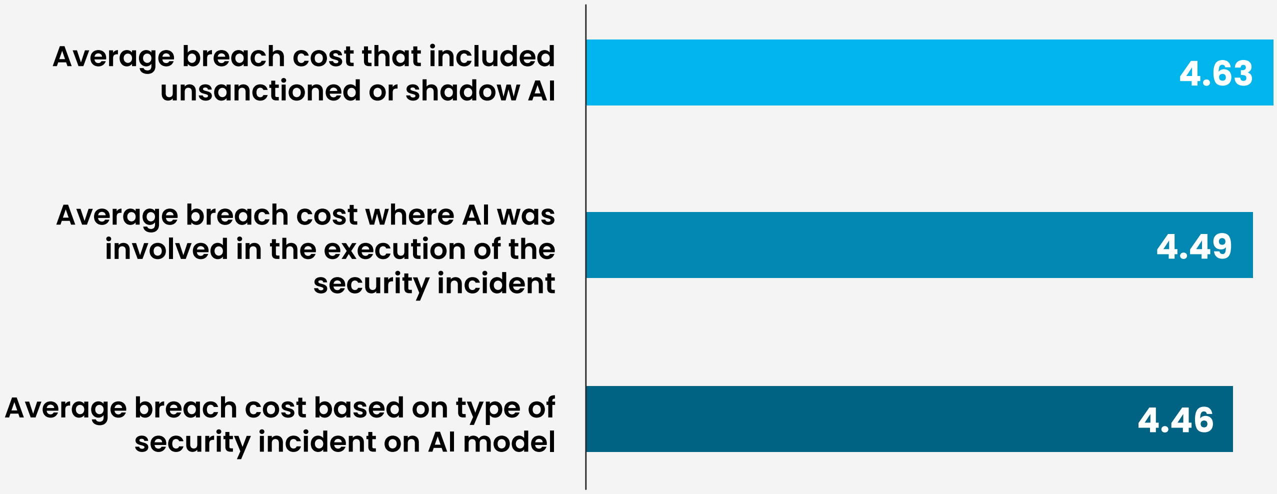
2. AI Introduces a New Era of Cyber Risk

AI tops the list of factors amplifying cyber risk – not only by enabling more sophisticated attacks, but also by expanding the attack surface as organizations rapidly integrate AI into their operations.

Some 87% of security professionals surveyed by SoSafe 2025 Cybercrime Trends[7] said their organization has encountered an AI-driven cyberattack in the last year, and 91% expect a significant surge in the coming years. Worse, AI attacks are triggering a bigger hit on company bottom lines:

Effect of AI on Data Breach Costs

Measured in USD millions



Source: IBM's 2025 Cost of a Data Breach report

Generative AI, in particular, has completely changed the game for cyberthreat actors. The prevalence of Large Language Models (LLMs) has lowered the barrier for entry into cybercrime in terms of cost and required expertise, making it far easier, faster, and cheaper to launch sophisticated attacks – at scale.

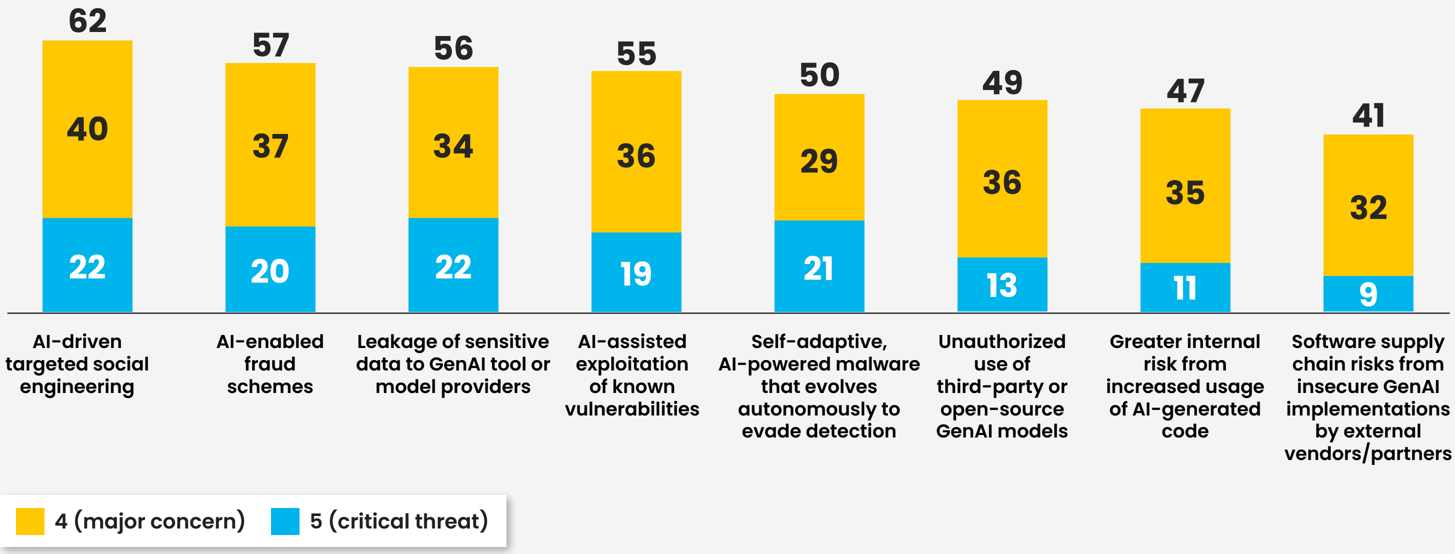
Cybercriminals leverage GenAI to convincingly replicate the communication styles of senior leaders at organizations, for example, fooling employees with phishing scams and deepfake impersonation attacks. GenAI is also used to develop credible social engineering attacks in a wide range of languages, helping threat actors target a greater number of people in more countries at a lower cost.

Nearly 47% of organizations rank adversarial GenAI as their top security concern – enabling adaptive malware, hyper-realistic deception, AI model manipulation, and large-scale attack automation, a 2025 World Economic Forum (WEF) cybersecurity survey[8] found. These advancements are tipping the scales in favor of cybercriminals – unless defenders match them with equally advanced, AI-powered countermeasures.

Top GenAI-Driven Concerns

% of Respondents

Q: On a scale from 1-5, how concerned are you about the following GenAI-related threats, including AI?



Source: BCG & GLG CISO 2025 survey[9]

But while an overwhelming majority (96%) of professionals surveyed by SoSafe recognize the importance of detecting AI-based attacks, only 26% rate their ability to do so as "high." This highlights a critical vulnerability: organizations are struggling to gain the budget and skills required to deploy the advanced AI tools needed to defend against AI-powered attacks.

Many IT teams still struggle to connect cybersecurity strategy with overall business goals – missing opportunities to gain executive alignment and secure adequate investment for critical initiatives (more on this later).

Meanwhile, business leaders have eagerly embraced AI integration, chasing quick returns and cost savings. Nearly 80% of organizations now use AI in at least one business function, up from 55% the previous year (McKinsey's State of AI 2025 report[10]).

This rapid adoption opens the door to new vulnerabilities. Many AI tools – whether third-party or custom-built – lack robust security safeguards, making them prime targets for cybercriminals.

Attackers can exploit these weaknesses to extract sensitive information, map network vulnerabilities, and bypass detection systems. IBM found that nearly one in three organizations that suffered an AI-related security incident experienced operational disruptions and data breaches, with 29% reporting data integrity losses (data becomes inaccurate, incomplete, or inconsistent).

Compounding the problem is the menace of shadow AI – employees using unauthorized AI tools for work. A robust "shadow AI economy" is flourishing under the radar at businesses, powered by employees using personal AI tools for day-to-day work.

MIT's State of AI in Business 2025 report[11] found that while only 40% of companies say they pay for official GenAI subscriptions, employees at more than 90% of firms regularly use personal AI tools such as ChatGPT or Claude on the job.

These unmonitored tools are proving to be costly: Shadow AI adds $200,000 to average breach costs and can extend containment times by a week, IBM found. High levels of shadow AI at an organization can add as much as $670,000 to a breach price tag, exposing more personal and proprietary data in the process.

Unsurprisingly, shadow AI has emerged as one of the top three costliest data breach factors, topped only by supply chain incidents and overly complex security system environments.

> **Shadow AI has emerged as one of the top three costliest data breach factors, topped only by supply chain incidents and overly complex security system environments. Security incidents involving shadow AI add $200,000 to average breach costs – and high levels of shadow AI can add $670,000.**
>
> *IBM's 2025 Cost of a Data Breach report*

3. Third-party Risk Becomes the Weakest – and Costliest – Link

Today, every business depends on a highly complex and interconnected ecosystem made up of supply chain vendors, technology providers, outsourcers, etc., to conduct its day-to-day operations. As Jeffrey Wheatman, Senior VP of Cyber Risk Strategy at Black Kite, said at a recent Auxis cybersecurity webinar[12], "No organization is an island unto itself."

In fact, SoSafe's survey revealed 93% of companies now rely on third-party services to deliver their main value proposition. This increased – and often unavoidable – dependence brings significant cybersecurity implications, dramatically widening your attack surface to not only include your direct vendors – but their entire supply chain as well.

Similarly, many organizations are rapidly adopting cloud technologies for their scalability, cost efficiency, and perceived security benefits. But while the cloud offers clear advantages, it also introduces new vulnerabilities – particularly when companies have limited control over configurations on Software-as-a-Service (SaaS) platforms.

Michael Hastings, Cybersecurity Advisor for the Department of Homeland Security, shared a telling example during the Auxis cybersecurity webinar:

"I was at an organization last week that said, 'We're good, all our data is secure, it's in the cloud.' But they didn't know where in the cloud, who had access to what applications, who was moving data, and what the security practices of their partners were. That was very concerning."

This lack of visibility creates a dangerous concentration of risk. A single attack on a major cloud provider – like recent attacks targeting AWS and Snowflake – could ripple across thousands of dependent businesses, halting operations overnight and leading to extensive short and long-term losses.

The scale of this problem is growing fast. The percentage of breaches involving a third party doubled in the last year, jumping from 15% to 30%, Verizon's 2025 Data Breach Investigations Report[13] found.

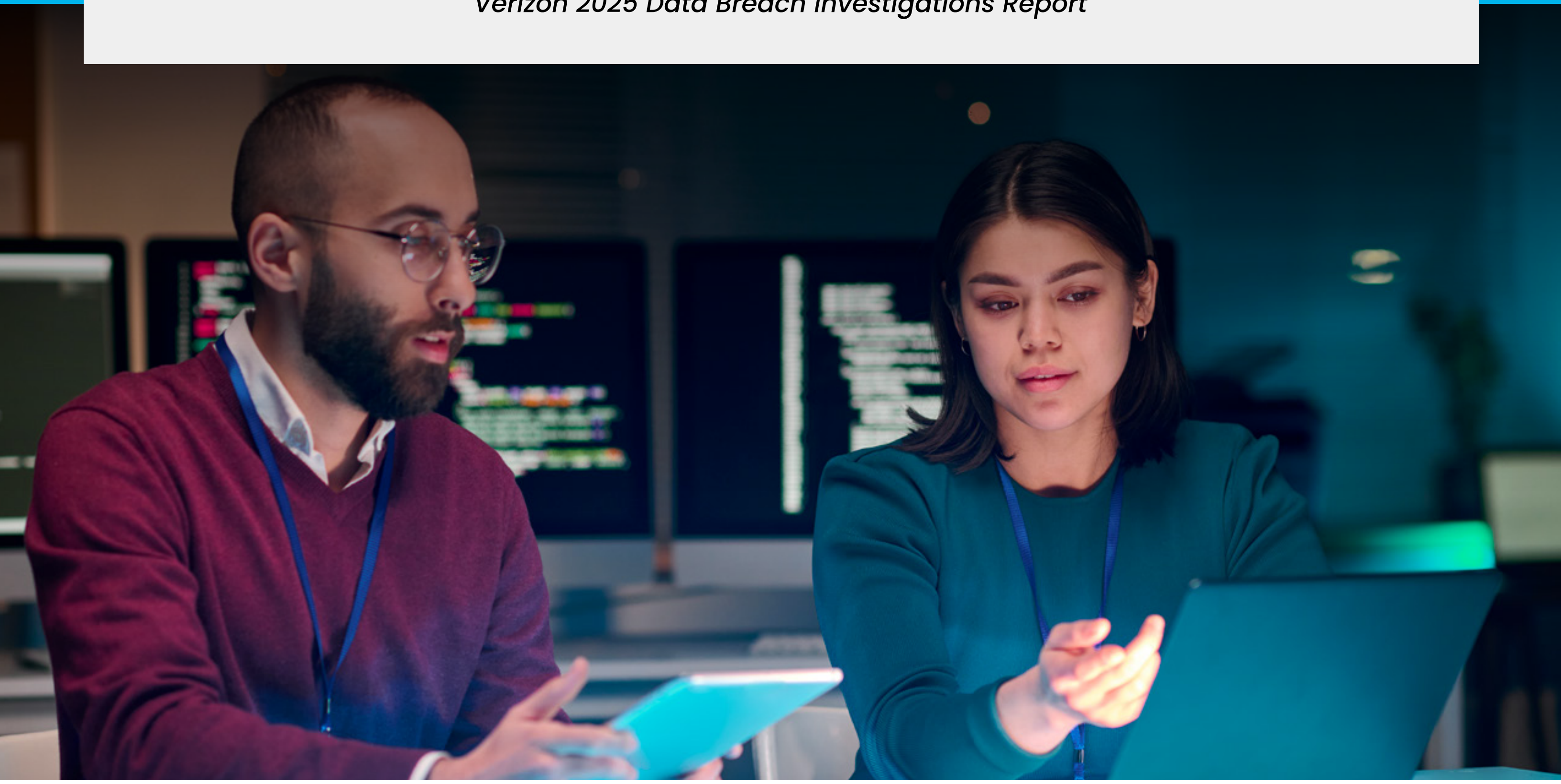
Even worse, at an average of 267 days, attacks on the supply chain also take the longest to detect and contain, IBM's data showed. This is because these attacks exploit the trust between vendors and customers, and automated system-to-system communications.

Delayed detection further stems from a lack of visibility and oversight into the security practices and embedded AI tools within suppliers' systems – expanding an organization's attack surface and risks multifold beyond what they can control.

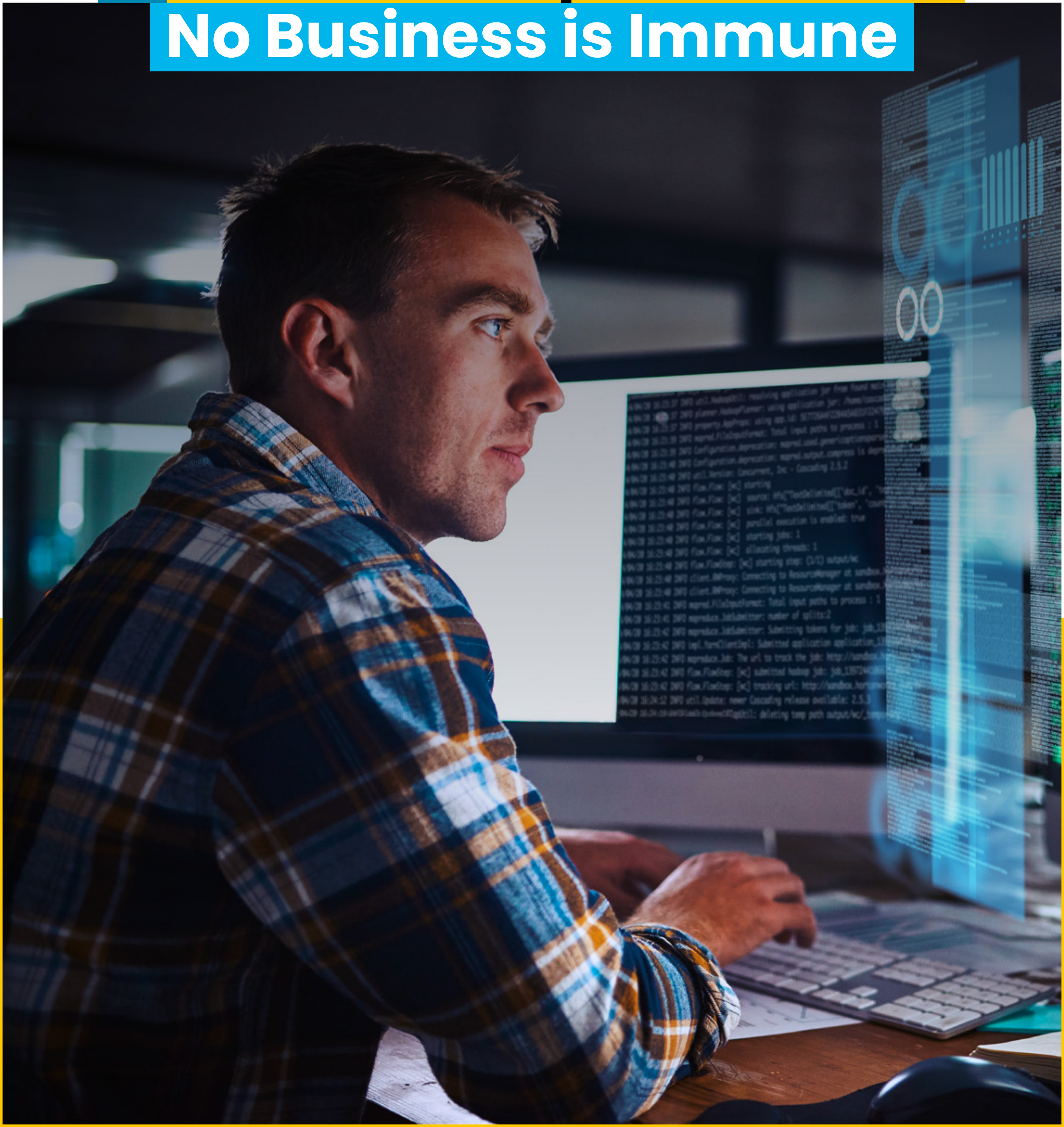
Put simply, in today's hyper-connected world, your business is only as secure as your weakest third-party link.

It follows then that 54% of large organizations surveyed by WEF cited supply chain vulnerabilities as the biggest barrier to achieving cyber resilience.

> **The percentage of breaches involving a third party doubled from 2024 to 2025, jumping from 15% to 30%.**
>
> *Verizon 2025 Data Breach Investigations Report*



4. From Startups to Giants, No Business is Immune



Today, no business, irrespective of its size, industry, or location, can say with certainty that it is safe from a cyberattack.

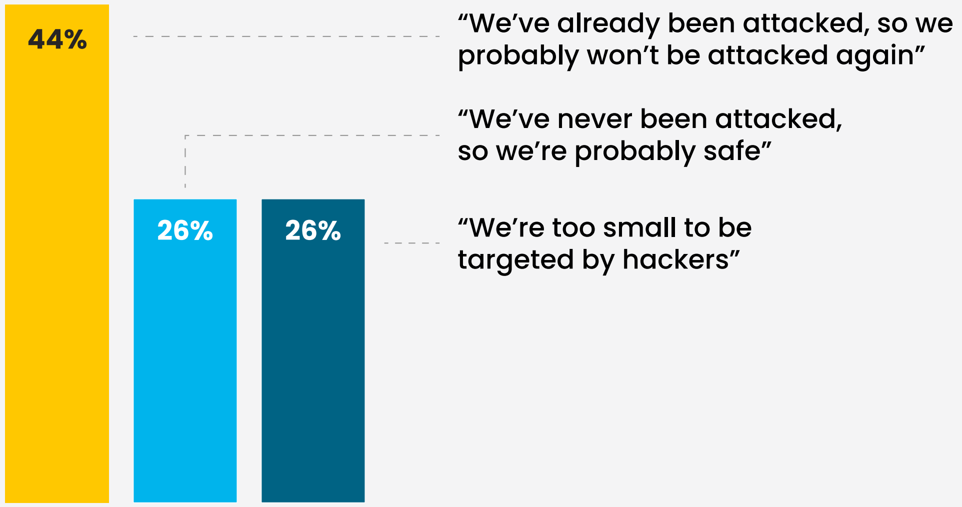
A decade ago, large enterprises and industries like retail and healthcare stood as the prime targets for cyberattacks – driven by their high ransom potential, valuable consumer data, and the notoriety associated with grabbing headlines. That is no longer the case today. In fact, as bigger corporations up their security game, threat actors have realized it is easier to penetrate smaller businesses with weaker defenses – and hitting several at once can add up to big payoffs.

> **One in three small and mid-size businesses (SMBs) experienced an attack in the preceding year, with attack costs running as high as $7 million.**
>
> *Microsoft SMB Cybersecurity Report 2024*

Ransomware, the dominant attack method for targeting businesses, disproportionally affects smaller organizations, Verizon found. Ransomware accounted for 88% of breaches at SMBs, compared to 39% for larger organizations.

Yet, many SMBs remain unaware of their heightened risk. The Microsoft study[14] revealed concerning mindsets at small and mid-size organizations that increase their cyber risk:

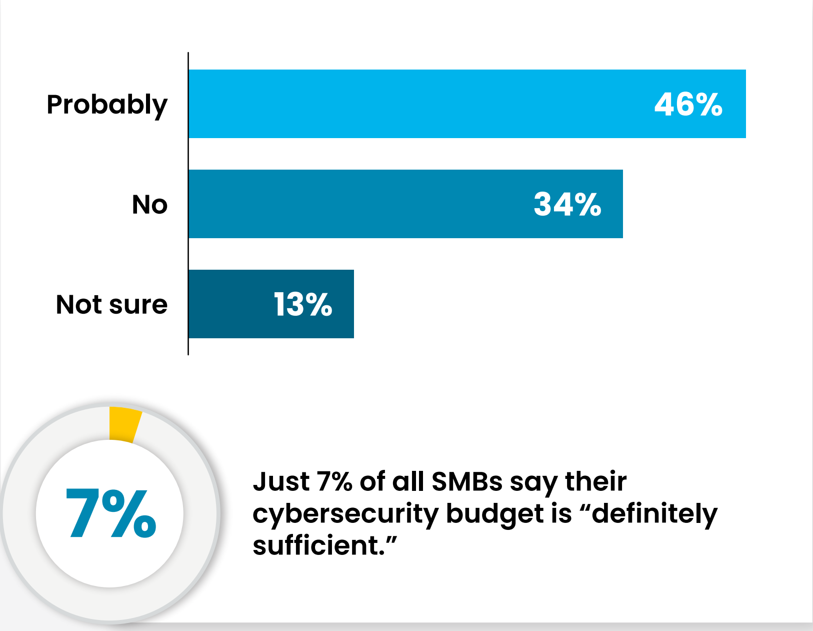
Insights into SMB Mindsets Regarding Cybersecurity



Source: Microsoft SMB Cybersecurity Report 2024

Yet, the biggest barrier to stronger cybersecurity at SMBs isn't lack of awareness, it's a lack of resources. Just 7% of small and mid-size organizations say their cybersecurity budget is "definitely sufficient," according to CrowdStrike's 2025 State of SMB Cybersecurity survey[15].

Budget Sufficiency



Just 7% of all SMBs say their cybersecurity budget is "definitely sufficient."

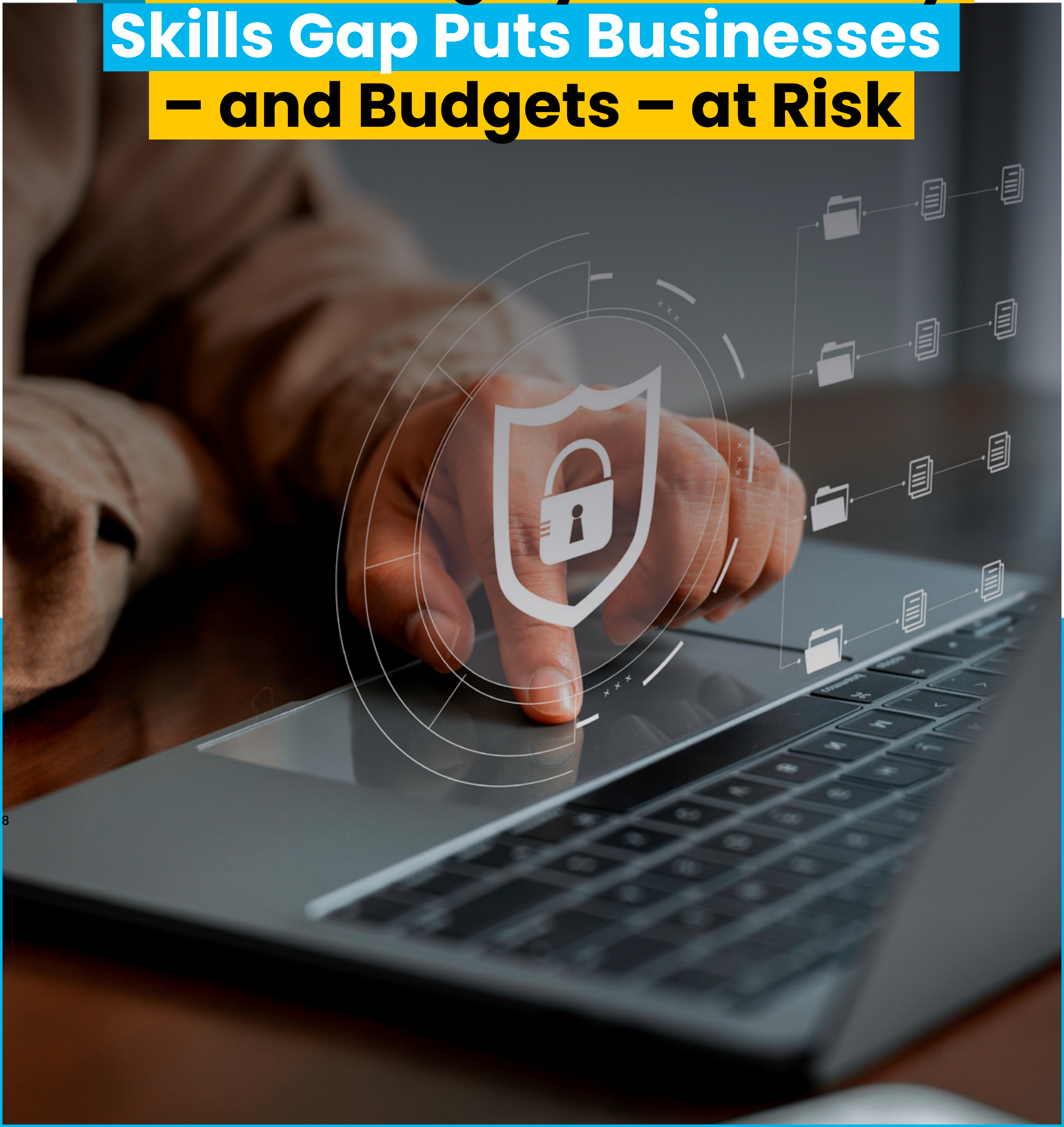
Source: CrowdStrike's 2025 State of SMB Cybersecurity survey

The global shortage of cybersecurity professionals – a trend we'll cover in more detail in the next section – adds to the problem. While well-funded sectors and bigger corporations can compete for top cybersecurity talent, smaller and under-resourced organizations often can't – leaving critical gaps in expertise and defense.

This imbalance triggers real-world consequences. Without robust recovery plans, backups, or cyber insurance, smaller businesses suffer the most in the event of a cyberattack.

Three-fourths of small businesses say a major cyberattack would "likely" or "definitely" put them out of business, CrowdStrike reported, compared to less than one-third of mid- and large-sized SMBs.

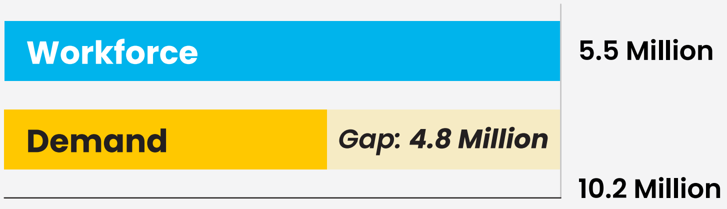
5. A Growing Cybersecurity Skills Gap Puts Businesses – and Budgets – at Risk



8

While the cybersecurity skills gap has persisted for about a decade, the shortfall has never been this severe. The 2024 ISC2 Cybersecurity Workforce Study[16] reports a staggering 4.8 million unfilled roles globally, even as the global cybersecurity workforce swelled to a record high of 5.5 million.

Global Cybersecurity Workforce Gap



Source: 2024 ISC2 Cybersecurity Workforce Study

In the U.S. alone, Cybersecurity Ventures[17] reports more than 750,000 cybersecurity job vacancies – pushing salaries higher as companies compete for a limited pool of talent.

Over the years, this skills gap has snowballed into a multi-faceted crisis – no longer just a headcount deficit, but a critical mismatch of skills and resources. Economic headwinds continue to tighten IT security budgets, leaving many organizations unable to hire – or competitively pay for – the talent they urgently need to protect their infrastructure.

The strain is especially visible in 2025, the IANS report found, with security leaders and their teams reporting they are stretched thin amid hiring freezes and limited budgets. Equally concerning is the widening skills gap – the lack of up-to-date capabilities and specialized knowledge – which is proving just as damaging as staffing shortages.

Organizations facing critical or significant skills gaps are almost twice as likely to experience a material breach compared to those without, the ISC2 survey report found. Nearly half of organizations that suffered a data breach reported grappling with severe cybersecurity talent shortages, the IBM report found.

The impact is costly: Organizations with a high level of skills shortages incur $5.22 million in average breach costs – a staggering $1.57 million more than organizations with a low-level or no skills shortage, IBM found.

AI is emerging as both a relief valve and a new source of pressure. On one hand, the accelerated adoption of AI tools is helping bridge skills gaps by improving threat detection, accelerating data processing, and enabling faster, more proactive remediation.

On the other hand, with AI adoption also prioritized across business operations, cyber professionals are already seeing more work: Over half of security teams surveyed by ISC2 have already faced data privacy and security concerns caused by organizational adoption of GenAI.

Most in-demand cybersecurity skills

While companies are hiring cybersecurity roles across the board, specialist cybersecurity skills are in the greatest demand as organizations confront sophisticated AI-powered attacks, rapid cloud adoption, stricter compliance and regulatory requirements, and the need to secure increasingly complex technology environments.

The most in-demand skills include:

Cloud computing

Cloud computing security ranks as the #1 sought-after technical skill, the ISC2 survey found. Hiring managers are seeking candidates experienced in:

- **Cloud platform and infrastructure security**
- **Cloud data security**
- **Cloud architecture and design**

Artificial Intelligence

AI offers a powerful opportunity to help close the widening cybersecurity skills gap. At the same time, AI adoption is generating new, specialized roles that demand advanced expertise. Hiring managers are looking for a new generation of cybersecurity professionals with skills spanning:

- **AI and machine learning (ML) models and model auditing**
- **Data science**
- **Natural language processing (NLP)**
- **Generative AI applications for cybersecurity**

Unfortunately, the workforce isn't quite ready. More than half of respondents to Ponemon's State of AI in Cybersecurity Report 2025 survey[18] view AI-powered tools as highly complex – and only 42% believe their cybersecurity teams are fully prepared to work with them.

Organizations are also prioritizing AI-related hires in security engineering, risk assessment, application security, governance, and risk management and compliance.

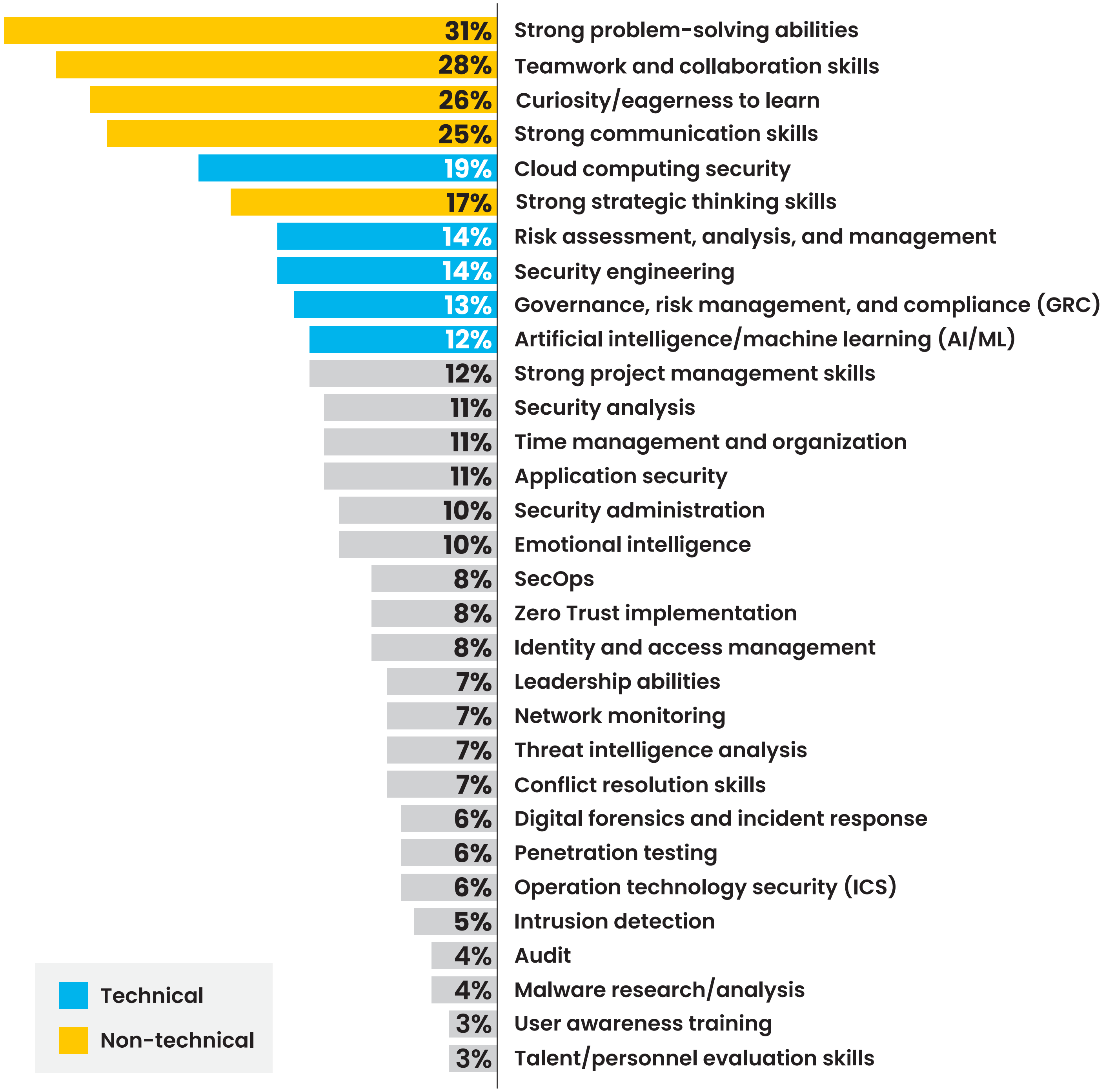
Non-technical skills

Beyond technical skills, hiring managers are prioritizing transferable soft skills that complement AI adoption. The top non-technical skills in demand today include strong problem-solving acumen, teamwork, collaboration, curiosity, and communication.

For hiring managers surveyed by ISC2, these skills ranked even higher than pure technical skills like cloud computing security and AI. The reason: They expect at least some specialized technical skills to be rendered obsolete by AI advances.

> **Only 42% of IT leaders say their cybersecurity teams are fully prepared to work with AI-powered tools.**
>
> *Ponemon's 2025 State of AI in Cybersecurity Report*

Ranking of Technical and Non-technical Skills by Hiring Managers



Source: ISC2 Cybersecurity Workforce Study 2024

6. Cybersecurity Becomes the #1 Outsourced Function – and Nearshoring Leads the Shift

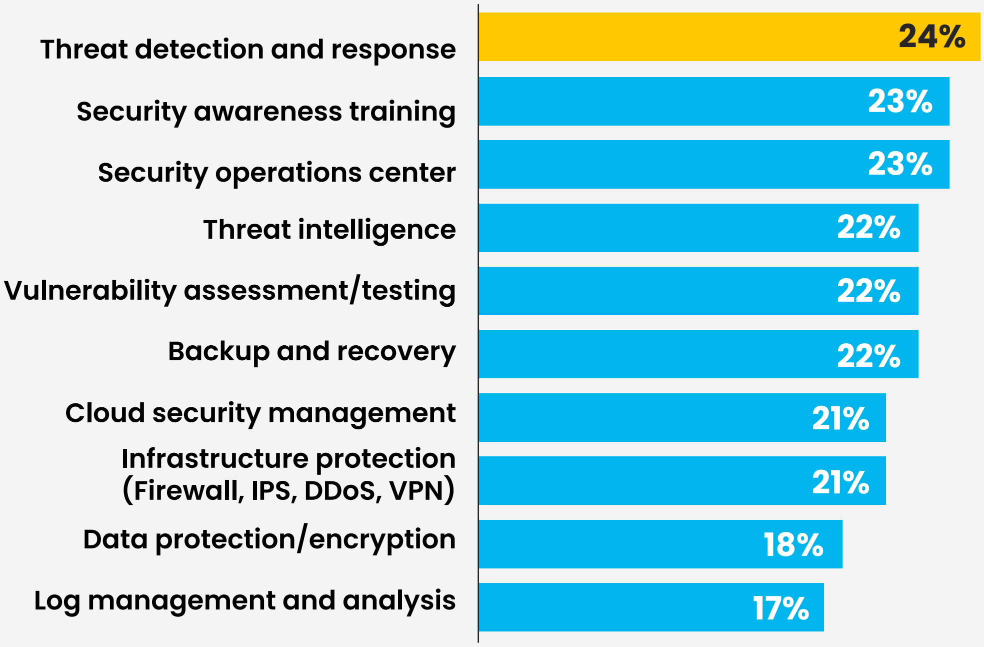
The cybersecurity landscape is evolving at breakneck speed – introducing new risks while intensifying long-standing challenges like talent shortages, skills gaps, and budget constraints.

To keep pace, most organizations have turned to external cybersecurity partners to strengthen their security posture and close internal capability gaps. Nearly 60% of organizations say they need outside expertise to maximize the value of AI-based security tools, Ponemon's report found.

The trend is accelerating rapidly. Cybersecurity, along with IT infrastructure services, stands as the #1 most-outsourced business function on Deloitte's 2024 Global Outsourcing Survey[19], with 77% of organizations now outsourcing at least part of their cybersecurity operations.

Foundry's 2024 Security Priorities study[20] reinforces this trend, revealing 82% of security decision-makers plan to outsource key cybersecurity functions to managed service providers (MSP) or other third parties in the next 12 months.

Security Functions Organizations Plan to Outsource



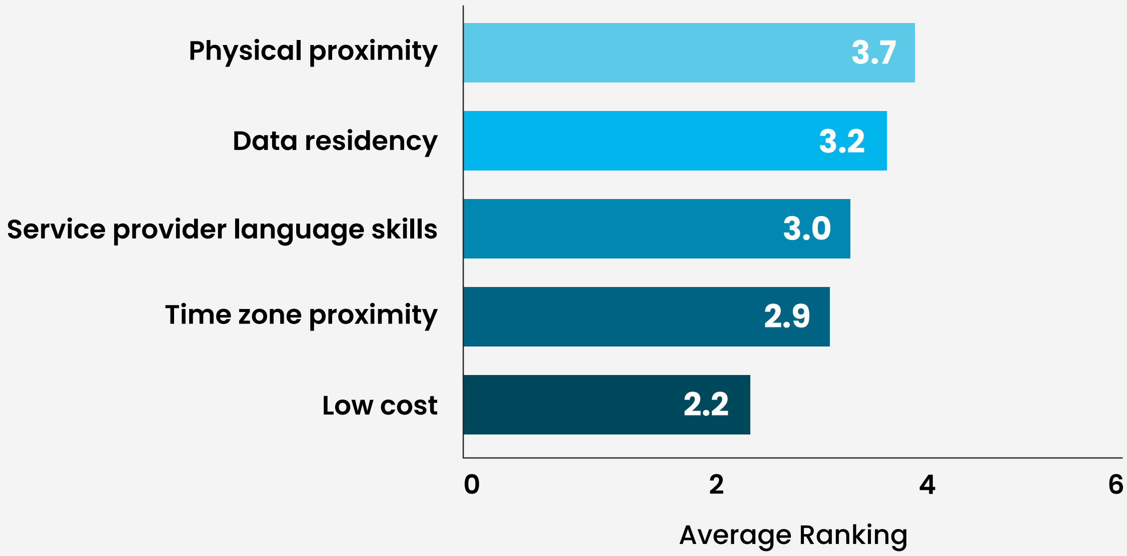
Question: Which of the following security functions will your organization outsource over the next 12 months to a managed security services provider or other third-party (not including SaaS)?

Source: CSO Security Priorities Study, 2024

But the reasons for choosing a security provider are changing. Amid labor challenges, "access to talent" eclipsed "cost reduction" as the #1 outsourcing driver for the first time since the pandemic, Deloitte found.

IT leaders narrow the selection process even more – ranking proximity, language fluency, and time zone compatibility as top reasons for choosing an IT outsourcing partner. Put simply, they are prioritizing smoother collaboration and fewer operational challenges – even if a lower cost can be realized in a more distant location, the latest IT Outsourcing Statistics Report by Computer Economics[21] found.

Most Important Attributes in Choosing a Service Provider



Source: Computer Economics

The advent of AI-powered automation is another major factor influencing location strategy. As AI automates many of the routine and repetitive tasks that once justified large delivery teams in low-cost locations, organizations are increasingly valuing partners with specialized expertise and strategic capabilities over pure cost advantages.

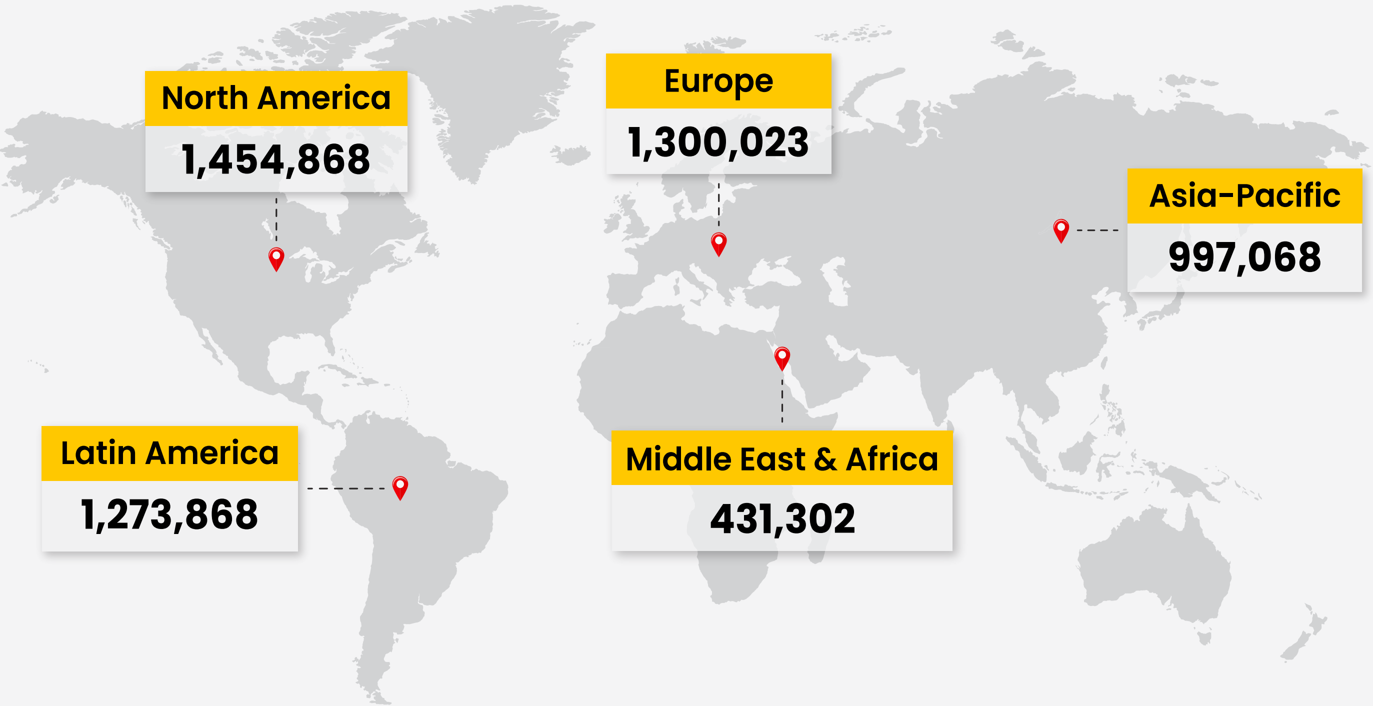
In this climate, Latin America has emerged as a leading destination for North American cybersecurity organizations, offering the agility, higher-value talent, and real-time collaboration needed to resolve urgent issues effectively.

With nearly 1.3 million professionals, Latin America offers one of the largest skilled cybersecurity workforces worldwide – outranking Asia's top outsourcing destinations and almost matching Europe's, according to the ISC2 study. In fact, Latin America ranks as the #1 up-and-coming tech talent market globally on CBRE's 2025 Scoring Tech Talent report[22] as ongoing investment from local governments and multinational corporations support a highly skilled, rapidly growing talent pool.

CBRE also notes tech labor costs in Latin America average 38% lower than the U.S. – enabling security organizations to optimize budgets without compromising quality.

Global Cybersecurity Workforce Estimate

5,457,173 +0.1% YoY



Source: ISC2 Cybersecurity Workforce Study 2024

Performance metrics tell the same story. Satisfaction levels at LATAM shared services organizations (87%) are significantly higher than Asia (53%), Europe (64%), and even North America (69%), according to the State of the GBS & Outsourcing Industry in Latin America report by SSON and Auxis[23].

Not surprisingly, LATAM SSOs are delivering IT processes like cybersecurity at nearly twice the global average (64% vs. 32%) – evidence of their capability, maturity, and rising strategic importance.

> **82% of security decision-makers plan to outsource cybersecurity functions to a managed service provider or other third-party in the next 12 months.**
>
> *Foundry's 2024 CSO Security Priorities Study*

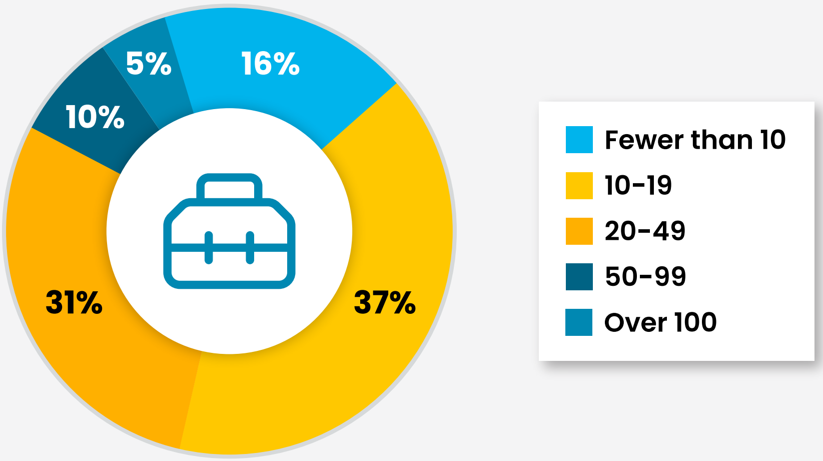
> **Latin America boasts a fast-growing workforce of about 1.3 million cybersecurity professionals, outranking Asia's popular outsourcing destinations.**
>
> *ISC2 2024 Cybersecurity Workforce Study*

7. Tool Overload and Alert Fatigue Undermine Cyber Resilience

Amid growing cyberthreats and expanding attack surfaces, security teams often confront another complexity: legacy security infrastructure. Struggling to work across dozens of disparate security solutions to secure an organization’s network, cloud, and endpoint environments, security teams are often left manually triaging alerts while fending off increasingly automated attacks.

Even as more robust security solutions become available, they often overlap with point solutions, leading to inefficiencies and the need for additional tools to fill gaps. Some 68% of organizations use between 10 and 49 security tools or platforms, the 2024 CDW Cybersecurity Report[24] found, with another 15% using even more tools!

Approximately How Many Security Tools/Platforms is your Organization Running?



Source: 2024 CDW Cybersecurity Report

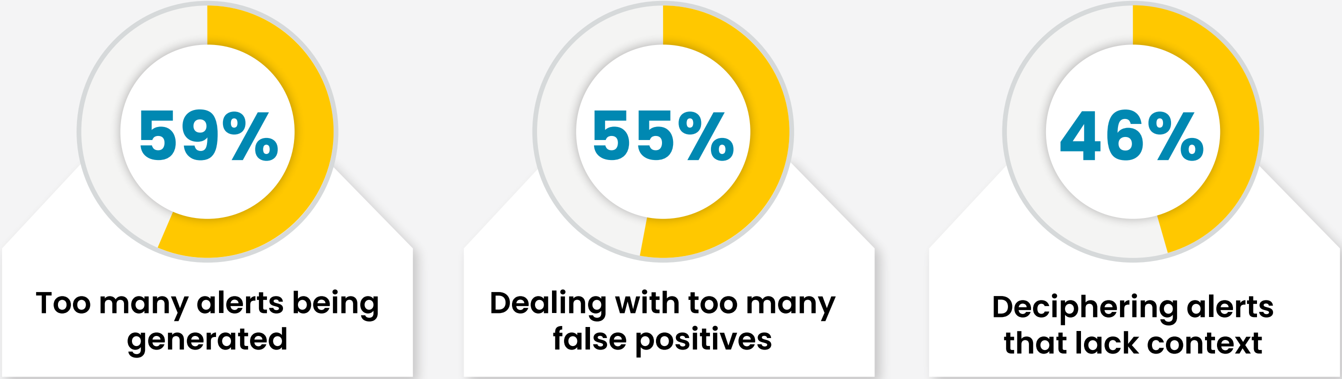
Worse, these tools are often difficult to integrate into the organization’s security environment. Nearly 80% of security leaders say their security tools are dispersed and disconnected, creating moderate to significant challenges for their team (Splunk’s 2025 State of Security report[25]).

Such challenges – ranging from illogical workflows to visibility gaps – add to the team’s stress and fatigue. Beyond inefficiencies, they fail to provide the integrated insights required for security teams to detect threats quickly and respond with speed and accuracy – instead creating information overload and an overwhelming number of alerts, leading to alert fatigue.

Security Operations Center (SOC) staff are overwhelmed by an average of 3,800+ alerts per day, a 2024 Vectra State of Threat Detection report[26] found. The result: 62% wind up ignored as security teams drown in excessive workloads – increasing the chance of real threats slipping by undetected.

False positives, which incorrectly indicate alerts suggest a threat, rank as another top concern, causing analysts to waste valuable time chasing phantom attacks – and potentially miss critical notifications.

Top Alerting Issues Creating Inefficiency for SOC Teams



Source: Splunk 2025 State of Security report

> **Tool sprawl creates significant inefficiencies: 68% of organizations use between 10 and 49 security tools or platforms, with another 15% using even more.**
>
> *CDW 2024 Cybersecurity Research Report*

8. AI vs. AI is the New Frontline in Today's Cyber Wars

Security teams are locked in an AI arms race – and it's driving a fundamental shift in how we protect our organizations. As traditional perimeter-based defenses fall short against AI-fueled threats, security teams are fighting back with intelligent, automated solutions that can detect, learn, and respond in real time.

The result is a new era in cybersecurity, where speed, adaptability, and machine intelligence are critical to staying ahead. Beyond strengthening defenses, these AI tools are also helping to close the widening cybersecurity skills gap and address many of the challenges that plague legacy security models.

Today, AI and machine learning account for 21% of the average IT security budget of $36.8 million, Ponemon found. The investment is only accelerating: Global spending on AI-powered cybersecurity is expected to jump from $31 billion in 2024 to $133 billion in 2030 (Technopedia AI Cybersecurity Insights[27]).

The impact of GenAI and Agentic AI

GenAI represents the biggest area of investment, used by nearly half (45%) of cybersecurity teams, the ISC2 report said. While top use cases involve automating operational processes and routine tasks like report writing and incident documentation, it is also increasingly being embedded into enterprise defense strategies.

In the U.S., about one in four SOCs leverage GenAI for cybersecurity defenses like threat detection (24%), development (23%), and querying security data (30%), Splunk reports. But those numbers are growing as AI-powered SOCs report measurable advantages, including faster alert resolution, improved resource allocation, real-time pattern recognition, and automatic documentation of complex processes.

Agentic AI – the latest and most autonomous form of AI – takes cybersecurity automation to the next level. Agentic AI empowers advanced software agents to learn, make decisions, and act independently, in concert with a governance model and human supervision.

By orchestrating the power of RPA, LLMs, API-driven coordination, and other advanced AI into an automated process, agentic automation can deliver defenses that are faster, more resilient, scalable, and increasingly proactive – automatically adapting to changing conditions and making intelligent real-time decisions.

While adoption is still in the early stages, 59% of security leaders say they are actively working to deploy Agentic AI, with real-world use cases already showing improved detection accuracy, faster response times, and higher SOC efficiency, according to the 2025 Cyber Security Tribe Annual Report[28].

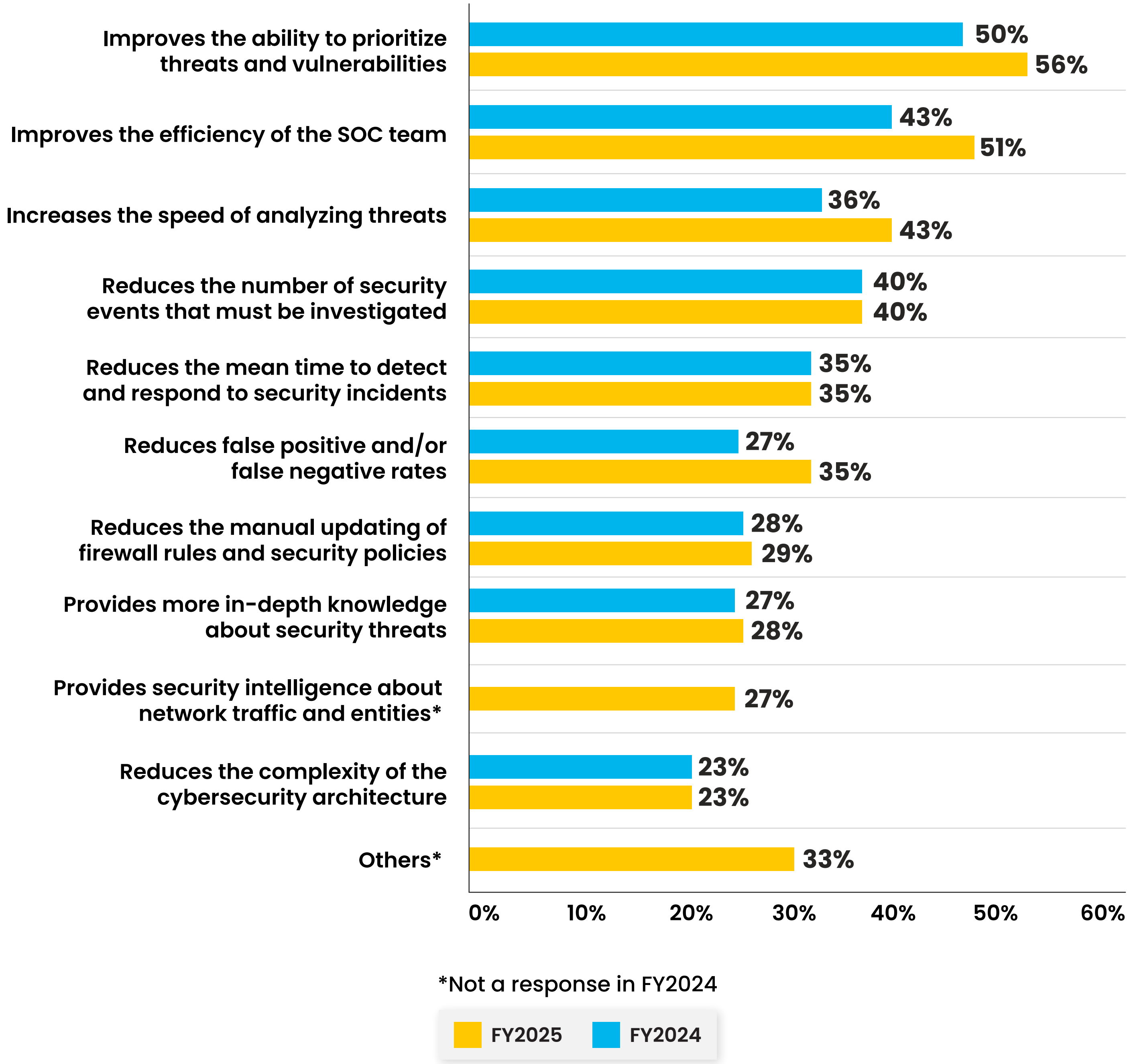
However, trust remains a challenge. Just 11% of cybersecurity leaders fully trust AI to handle mission-critical SOC activities, Splunk found – citing concerns about data accuracy, privacy, and compliance.

Maintaining a human-in-the-loop strategy, supported by robust governance and compliance frameworks, is essential to building confidence in these emerging technologies.

Here’s the bottom line: AI cannot replace the human element in cybersecurity – but it can significantly amplify it. AI brings speed, scalability, and pattern recognition, while human analysts contribute context, intuition, oversight, and ethical judgment.

Success rests on building a workforce capable of harnessing the power of AI effectively – strengthening defenses and connecting technical actions to business results. It’s no surprise 87% of IT leaders are turning to outsourcing to accelerate AI adoption in critical areas like security – gaining access to the tools, tech, and expertise they lack in-house (Deloitte).

How Does AI Improve your Organization's Security Posture?



Source: State of AI in Cybersecurity Report 2025, Ponemon Institute

> **59% of security leaders are actively working to deploy Agentic AI, with real-world use cases already showing improved detection accuracy, faster response times, and higher SOC efficiency.**
>
> *2025 Cyber Security Tribe Annual Report*

> **Just 11% of cybersecurity leaders fully trust AI to handle mission-critical SOC activities.**
>
> *Splunk 2025 State of Security Report*

Top AI-powered capabilities CISOs are adding to their arsenal

Rapid threat detection

AI can spot subtle anomalies and attack patterns in real time that human analysts would likely miss – cutting detection time from weeks to minutes. It's especially invaluable for zero-day threats, insider risks, and GenAI-powered phishing.

70% of security professionals say AI has proved highly effective for detecting threats that previously would have gone unnoticed (Ponemon).

Automated incident response

AI can autonomously execute response playbooks – quickly isolating devices, blocking malicious IP addresses, and triggering recovery to minimize manual effort and breach impact.

AI users cut breach costs by $1.9 million and response time by 80 days (IBM).

Powerful phishing detection

With more than 40% of phishing emails now AI-generated (VIPRE Q2 2024 Email Threat Trends Report[29]), savvy security leaders are leaning on LLMs to fight back: quickly analyzing language, sender reputation, and contextual clues to proactively block sophisticated phishing attempts.

AI models reach up to 97.5% accuracy in phishing detection – even when messages appear legitimate to human analysts (Gartner[30]).

Smarter prioritization and remediation of vulnerabilities

AI can correlate threat intel with your specific infrastructure to identify which vulnerabilities matter most – and how to fix them.

45,500 new vulnerabilities were expected in 2025 – making it essential to focus your resources on the greatest risk (Forum of Incident Response and Security Teams[31]).

Predictive threat intelligence

By analyzing historical attack patterns, current threat intelligence, and environmental factors, AI can forecast attack vectors before they hit, enabling proactive defense.

GenAI simulates realistic threats, can detect zero-day vulnerabilities before they're known, and is helping classify new malware strains capable of mutating to evade detection.

Automatic alert response and triaging

AI filters the noise so stretched security teams can focus on high-priority threats – for instance, prioritizing threats and vulnerabilities, closing false positives, correlating data for a holistic view, and tackling low-risk alerts.

59% of organizations say AI significantly or moderately boosts security efficiency (Splunk).

9. AI Adoption Outpaces AI Governance

AI-related privacy and security incidents surged 56.4% in 2024 over the previous year, according to the 2025 Stanford AI Index Report[32]. As AI becomes more deeply embedded in security operations, strong governance, transparency, and ethical oversight are no longer optional – they're essential to mitigating risks.

However, while AI adoption is rapidly progressing among businesses of all sizes, shadow AI is spreading just as fast – and governance is struggling to keep pace. Nearly two-thirds of organizations (63%) surveyed by IBM admit they don't have AI governance policies in place to manage AI or detect shadow AI.

In the race to create value from GenAI investments, innovation is taking precedence over security. Only 24% of current GenAI projects include any security component, a recent IBM study of C-suite executives[33] found, even though 82% of respondents say secure and trustworthy AI is critical to business success.

It's a dangerous gap: Among organizations that reported AI-related breaches, 97% lacked proper access controls and governance, IBM's Data Breach Report found. Even when governance policies exist, less than half have formal approval processes for AI deployments, and 61% lack the technologies needed to enforce AI governance effectively.

The result: AI adoption is racing ahead, largely unchecked. The consequences are serious – ranging from data leakage and prompt injection to model manipulation, identity exploitation, and unauthorized access. Each carries steep financial, reputational, and trust costs.

Primary GenAI Security Risks, Threats, and Challenges

- Prompt injection attacks
- AI system and infrastructure security
- Insecure AI-generated code
- Data leakage and exposure
- Data poisoning
- AI supply chain vulnerabilities
- Shadow AI
- Access and authentication exploits
- Adversarial inputs and evasion
- Model inversion and extraction attacks (reconstructing sensitive input data from an AI model or stealing its structure/parameters)
- Model drift and performance degradation due to changes in data or user behavior
- Risks from third-party tools, libraries, or pre-trained models integrated into GenAI systems
- Lack of algorithmic transparency and explainability
- Unauthorized access and misuse
- Lack of auditability and traceability

As more advanced types of AI like Agentic AI find traction among businesses, the need for strong governance, transparency, and ethical oversight becomes even more urgent. These measures are essential for ensuring responsible deployment, preventing unintended consequences, and safeguarding against misuse, bias, and security vulnerabilities.

Regulation and governance serve as important drivers of cyber resilience: 78% of CISOs and 87% of CEOs cite improving security posture and mitigating cyber risks as their top motivations for embracing new cybersecurity regulations, the WEF survey found.

Yet, implementing these measures is not without challenges. Nearly 70% view cybersecurity regulations as overly complex or burdensome – or struggle to verify third-party compliance, the WEF survey found.

At the same time, regulatory pressure is rising: U.S. federal agencies introduced 59 AI-related regulations in 2024 alone (Stanford AI Index). As government and industry bodies accelerate oversight, many companies worry about regulatory fatigue – meaning the sheer volume and pace of new rules could overwhelm security teams and dilute the intended impact of the frameworks.

> **Only 24% of current GenAI projects include any security component, even though 82% of respondents say secure and trustworthy AI is critical to business success.**
>
> *IBM Institute for Business Value study*

10. The ROI Challenge Redefines Cybersecurity Strategy

As cyberattacks grow more frequent and costly, security leaders face mounting pressure to justify their cybersecurity investments. Yet proving return on investment (ROI) remains one of the biggest challenges for security teams.

After all, when success means preventing incidents that never happen, value is hard to quantify in traditional business terms. Unfortunately, that leaves many organizations unable to secure budget for proactive defenses – and exposed to greater losses when breaches occur.

As a result, forward-thinking security leaders are reframing their mindsets – shifting from a prevention-only strategy to one focused on cyber resilience. This means adopting a "when, not if" mentality that accepts the inevitability of attacks in the era of AI – and focuses on early detection, minimizing impact, rapid recovery, and adapting to future threats.

A key part of this shift rests on investing in pre-emptive, AI-powered security tools such as endpoint protection platforms and threat intelligence technology to stop breaches fast and prevent future attacks. More than 40% of U.S. IT security practitioners said their organizations have adopted pre-emptive security measures, Ponemon reports.

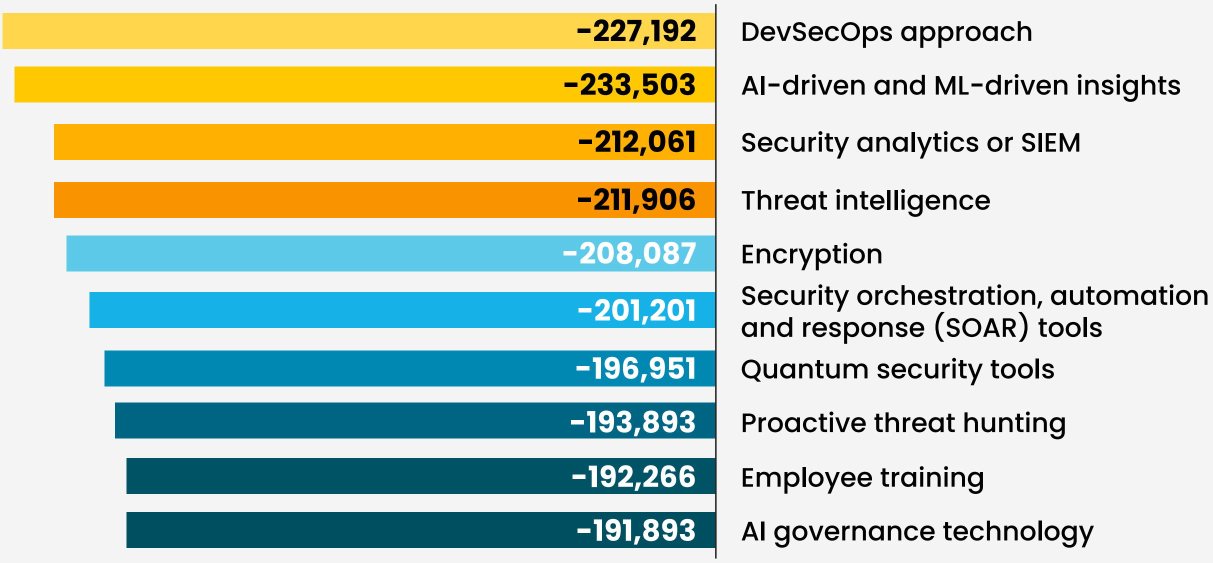
These tools help:

- Deter threats and minimize damage, focusing resources on the highest business risks.
- Guide response teams with insights into attack objectives and potential targets.
- Continuously improve forecast accuracy through adaptive learning.
- Reduce costs associated with handling attacks.

These proactive threat hunting tools can shave off almost $200,000 from average breach costs, IBM found.

The Top 10 Security Investments that Lower Data Breach Costs

Cost difference from last year's $4.88 million global breach average, measured in $



Source: IBM's 2025 Cost of a Data Breach report

Still, quantifying the business impact of these security investments to the C-suite remains a major hurdle. Fewer than half of C-suite executives say CISOs are significantly involved in planning cybersecurity investments or overseeing tech deployments at their organization, PwC's 2025 Global Digital Trust Insights[34] found.

This often leads to misaligned priorities and weaker security stances, as cybersecurity decisions may be made without proper risk assessment, business context, or operational readiness.

Here's the takeaway: Cybersecurity doesn't generate revenue – it protects it. So, proving cybersecurity return on investment (ROI) requires a different lens.

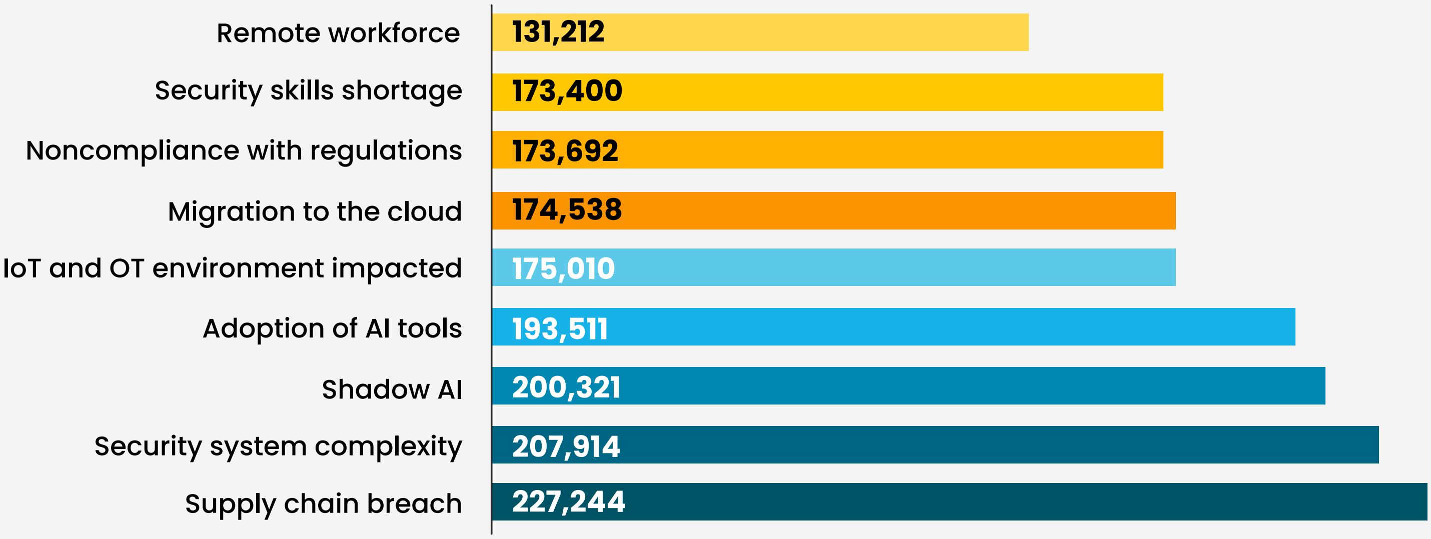
Instead of measuring revenue gained, the most effective method for calculating cybersecurity ROI involves comparing the costs of strengthening your defenses with the potential financial, reputational, and operational losses of a successful cyberattack.

$$\frac{(\text{Annual Cost of Security Incidents Avoided} - \text{Annual Security Investment})}{\text{Annual Security Investment}} \times 100 = \text{ROI}$$

With average data breach losses surpassing $10 million in the U.S., the best cybersecurity business case comes down to quantifying risk avoided and resilience gained.

Top Drivers of Data Breach Costs

Cost difference from last year's $4.88 million global breach average, measured in $



Source: IBM's 2025 Cost of a Data Breach report

> **Fewer than half of C-suite executives say CISOs are significantly involved in planning cybersecurity investments or overseeing tech deployments at their organization.**
>
> *PwC's 2025 Global Digital Trust Insights*

Cyber resilience begins with the right partner

2026 marks a defining moment for enterprise defense – and security leaders face a dual challenge: managing an expanding threat surface and rapid-fire AI attacks while navigating skills gaps, wide coverage requirement, regulatory complexity, and budget pressures. The cybersecurity trends shaping 2026 make one thing clear – resilience, not prevention alone, defines cyber maturity.

As the ongoing talent shortage continues to test the limits of internal security teams, CISOs and CIOs are rethinking their operating models – driving greater reliance on AI-powered automation and trusted managed security services partners (MSSPs) to close capability gaps and strengthen response.

Nearshoring to Latin America is becoming central to modern cyber strategies – delivering certified cybersecurity talent aligned by time zone, culture, and collaboration style to achieve enterprise-grade protection, sustainable cost efficiency, and faster response.

In a world where cyber risk never sleeps, partnering with a leading nearshore MSSP like Auxis gives organizations instant access to turnkey security operations, strategic guidance, and best practices without the cost and headache of building extensive security operations in-house.

The result: the ability to harness the latest cybersecurity trends to move beyond reactive defense – building proactive, adaptive, and resilient security capabilities that stay ahead in the era of AI threats.

Want to learn more about the latest cybersecurity trends or the benefits of managed security services?
Contact our cybersecurity experts today!

Or, visit our resource center for more cybersecurity tips, strategies, or success stories.

About Auxis

Now part of Grant Thornton U.S., **Auxis** is a leading consulting and tech-enabled nearshore outsourcing pioneer focused on helping organizations achieve a competitive edge through innovative processes, leading technologies, and world-class shared services. Fortune 1000 and upper-middle-market organizations have relied on Auxis' customized solutions since 1997 to obtain real benefits and ROI from their transformation programs.

Auxis delivers comprehensive solutions to modernize and scale business operations across Cybersecurity, IT, Finance, HR, Customer Service, and industry-specific functions including Revenue Cycle Management in Healthcare, Loan Processing, and Restaurant Store Audits. Its nearshore delivery platform is supported by award-winning Digital Transformation capabilities spanning Intelligent Automation & RPA, AI, Agentic, Analytics, and Cloud. A nearshore outsourcing pioneer, Auxis is consistently recognized as a top outsourcing company globally by respected analysts and industry organizations including Everest Group, ISG, and IAOP.

Auxis is headquartered in Fort Lauderdale, Florida, with main delivery centers in Costa Rica and Colombia, and supporting hubs in Mexico and Guatemala.

About Grant Thornton

Grant Thornton delivers professional services in the U.S. through two specialized entities: Grant Thornton LLP, a licensed, certified public accounting (CPA) firm that provides audit and assurance services and Grant Thornton Advisors LLC (not a licensed CPA firm), which exclusively provides non-attest offerings, including tax and advisory services.

In January 2025, Grant Thornton Advisors LLC formed a multinational, multidisciplinary platform. The platform offers a premier advisory and tax practice, as well as independent audit practices. With offices across the Americas, Europe and the Middle East, the platform delivers a singular client experience that includes enhanced solutions and capabilities, backed by powerful technologies and a roster of 15,000 quality-driven professionals enjoying exceptional career-growth opportunities and a distinctive cross-border culture.

Grant Thornton is part of the Grant Thornton International Limited network, which provides access to its member firms in more than 150 global markets.

Grant Thornton LLP, Grant Thornton Advisors LLC and their respective subsidiaries operate as an alternative practice structure (APS). The APS conforms with applicable laws, regulations and professional standards, including those from the American Institute of Certified Public Accountants.

"Grant Thornton" refers to the brand under which the member firms in the Grant Thornton International Ltd (GTIL) network provide services to their clients and/or refers to one or more member firms. Grant Thornton LLP and Grant Thornton Advisors LLC serve as the U.S. member firms of the GTIL network. GTIL and its member firms are not a worldwide partnership and all member firms are separate legal entities. Member firms deliver all services; GTIL does not provide services to clients.

Content Contributor

Sruthi Ramakrishnan
Content Marketing Specialist
Auxis

External Source Footnotes

1. Allianz, “Allianz Risk Barometer: Identifying the major business risks for 2025” January 2025
2. Check Point, “The State of Cyber Security 2025” January 14, 2025
3. Gartner, “3 Key 2025 Imperatives for Security and Risk Management” March 28, 2025
4. IANS, “IANS Security 2025 Budget Benchmark Report” August 14, 2025
5. IBM, “2025 Cost of a Data Breach” July 30, 2025
6. Check Point Research, “Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions” July 17, 2025
7. SoSafe, “SoSafe’s 2025 Cybercrime Trends” March 6, 2025
8. World Economic Forum, “Global Cybersecurity Outlook 2025” January 13, 2025
9. BCG, “BCG & GLG CISO Survey” July 30, 2025
10. McKinsey, “The state of AI” March 5, 2025
11. MIT NANDA, “The GenAI Divide: State of AI in Business 2025” July 2025
12. Auxis, “Unveiling the Latest Threat Intelligence: Practical Strategies for Strengthening Your Security Posture in 2025” July 30, 2025
13. Verizon Business, “2025 Data Breach Investigations Report” April 23, 2025
14. Microsoft, “SMB Cybersecurity Research Report” October 31, 2024
15. CrowdStrike “2025 State of SMB Cybersecurity Report” May 5, 2025

16. ISC2, “2024 ISC2 Cybersecurity Workforce Study” October 31, 2024

17. Cybersecurity Ventures, “2023 Cybersecurity Jobs Report” April 14, 2023

18. Ponemon Institute, “State of AI in Cybersecurity Report 2025” June 9, 2025

19. Deloitte, “Global Outsourcing Survey 2024” June 2024

20. Foundry's CSO, “2024 Security Priorities Study” October 23, 2024

21. Computer Economics (Avasant Research), “IT Outsourcing Statistics – Outsourcing Trends and Cost/Service Experiences for 11 Key IT Functions” April 2023

22. CBRE, “Scoring Tech Talent 2025” September 9, 2025

23. SSON, “State of the GBS & Outsourcing Industry in Latin America” September 26, 2024

24. CDW, “2024 CDW Cybersecurity Research Report” June 3, 2024

25. Splunk, “State of Security 2025: The Stronger, Smarter SOC of the Future” May 20, 2025

26. Vectra AI, “2024 State of Threat Detection and Response Report: The Defenders’ Dilemma” October 3, 2024

27. Technopedia AI Cybersecurity Insights, 2024

28. Cyber Security Tribe, “Annual State of the Industry Report 2025” December 4, 2025

29. VIPRE Security Group, “Q2 2024 Email Threat Trends Report” July 31, 2024

30. Gartner, “Gartner Identifies the Top Cybersecurity Trends for 2025” March 3, 2025

31. Forum of Incident Response and Security Teams, “Vulnerability Forecast for 2025” February 25, 2025

32. Stanford Institute for Human-Centered AI, “The 2025 AI Index Report” April 18, 2025

33. IBM Institute for Business Value study of C-suite executives, 2023

34. PwC, “PwC 2025 Global Digital Trust Insights” September 30, 2024

auxis

A Grant Thornton US company

www.auxis.com