HCLTech | Supercharging Progress™

The Global **Cyber Resilience** Study 2024-25

Intro **Note**

In today's ever-shifting cybersecurity landscape, resilience is more crucial than ever. Organizations must tirelessly build a robust and dynamic cybersecurity posture as cyberattacks grow in frequency and sophistication. Our latest Global Cyber Resilience Study reveals that over half of security leaders have experienced cyberattacks in the past year.

Alarmingly, three-quarters of these organizations faced substantial hurdles in recovering from these incidents, highlighting the need to build better recovery and response mechanisms and testing the same regularly.

As we look to the near future, two-thirds of security leaders expect a cyberattack on their organization in the next 12 months, with AI-generated attacks emerging as a top concern. This is a moment for decisive management action: enhancing communication about cybersecurity with the C-suite and board, closing the skills gap through partnerships with trusted service providers and ensuring every cybersecurity investment delivers real, measurable benefits that enhance business speed and align with broader business goals. This report isn't just a snapshot of where we are today—it's also a directional input to where we need to go next. By analyzing different industries and global regions, we've gathered insights highlighting the unique challenges and priorities across sectors, enabling us to offer more tailored recommendations. Security leaders are focusing on key areas such as cost optimization through automation and efficiencies, consolidating products into broader platforms, automating SOC operations, ensuring real-time risk management and building strong incident response and recovery plans.

This approach will empower organizations to establish and maintain a cybersecurity posture with robust prevention, response and recovery capabilities.

The report also showcases how security leaders embrace GenAI to secure business GenAI initiatives, driving progress toward building a resilient organization. We hope this report's insights are valuable as you continue your journey toward a more secure and resilient future. Enjoy the read!

Jagadeshwar Gattu

President, Digital Foundation Services, HCLTech

Amit Jain

Global Head, Cybersecurity Services, HCLTech

Executive Summary

In today's rapidly evolving landscape, global conflicts, economic headwinds, elections and emerging technologies like GenAI create new headwinds, making organizations more prone to cyberattacks. Adding to these challenges, security leaders must also navigate the pressures of growing industry and geo regulations and the widespread digital transformation reshaping many industries. For CISOs, the path forward requires wearing multiple hats and a strong focus on bolstering risk management through visibility and response capabilities, leaning into automation and MDR (Managed Detection and Response) for faster recovery and ensuring compliance amid rising regulatory demands. Closing skill gaps, partnering with trusted providers and aligning cybersecurity investments with digital transformation goals will be vital to staying resilient in this dynamic cybersecurity landscape.

The report underscores the pressing need for organizations to evolve their cybersecurity strategies, improve preparedness and build resilience against increasingly sophisticated threats.

The new normal: Target is everyone

In the past year, over half of the security leaders (57%) faced the reality of a cyberattack, differing in size, scale and intensity, with businesses in North America experiencing the highest (64%) and industries like Life Sciences and Healthcare (62%) bearing the biggest brunt. Attackers used cloud malware injections, credential theft and API vulnerabilities to wreak havoc, stretching recovery efforts thin. Returning to normal operations was an uphill battle for many—nearly three-quarters of security leaders reported moderate to severe difficulties, especially in Telecom, Media and Entertainment. The future looks no easier: 81% of leaders expect to be hit again in the next 12 months, with AI-generated threats becoming a growing concern.

Confidence score and CISO focus

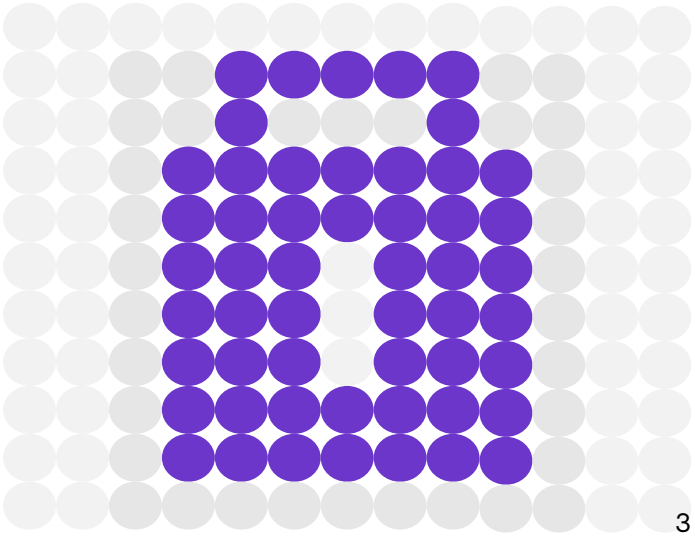
Many organizations are still playing catch-up when it comes to cyber readiness. Only 48% of security leaders feel confident in preventing attacks, and just 46% believe they are prepared to respond and recover effectively against a sophisticated attack. The inhouse expertise needed to tackle these growing threats is also lacking—just 35% of leaders say they have enough resources to deal with current cybersecurity risks. This is particularly concerning for sectors like Financial Services, Healthcare and Retail, where better incident response, governance and communication practices are critical.

Strategic priorities and budget investments

In response to these growing threats, security leaders are focused on optimizing cybersecurity costs, streamlining security platforms and embracing architectures like Zero Trust. While 2024 was managed with a lot of budget restrictions, most security leaders expect budgets and investments to increase by an average of 11% in 2025, with investments being funneled into improving risk management and compliance, SOC automation, incident response and building stronger cyber resilience. Industries like Life Sciences, Healthcare and Financial Services are leading the way in these efforts. Some of the new investments will also be self-funded through efficiency and vendor consolidation-driven savings.

Outsourcing and MSSP partnerships

Many organizations are turning to managed security service providers (MSSPs) to support their cybersecurity, and 90% rely on these partnerships to also achieve some of the above strategic priorities. As organizations reevaluate their current partnerships, the focus shifts from cost to consolidation capabilities and global scale, reflecting a more robust demand for modern outcome-based, sustainable and reliable outsourcing.



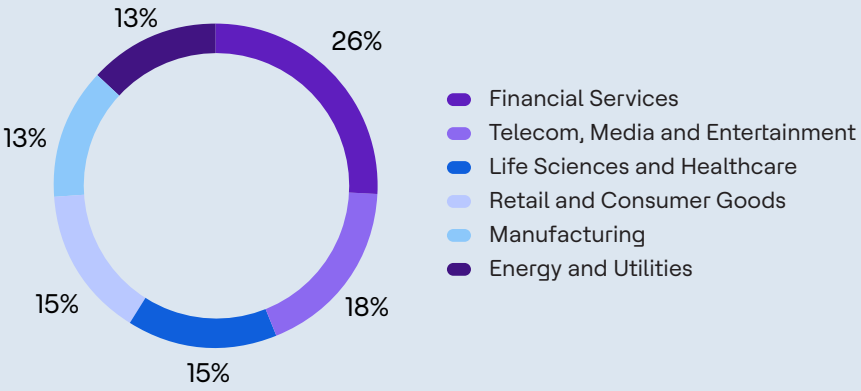
Scope of research

This research study is independently conducted by Ponemon Institute LLC and sponsored, analyzed and published by HCLTech.

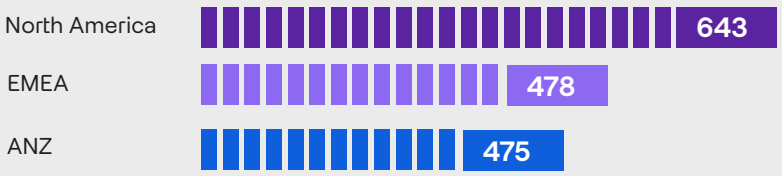
1,596

surveyed security leaders who are the primary decision makers or influence decision-making related to cybersecurity in their organization

Respondents by Industry



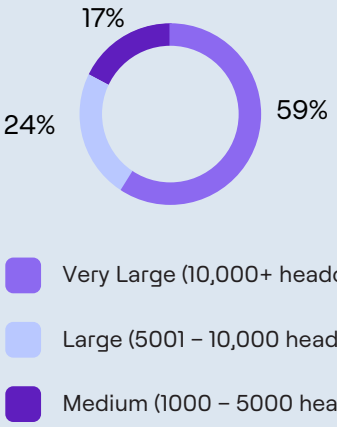
Respondents by Region



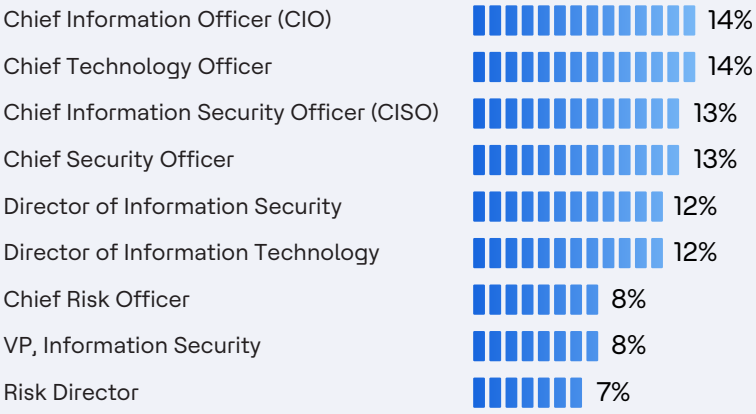
100%

surveyed are C-suite or influence cybersecurity decision-making

Respondents by Enterprise Size



Respondents by Current Title



About Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.
We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from Individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Report Agenda

1 The new normal of acceptance: Target is everyone

- Attack economy: Growing reach, volume and frequency
- Top concerns across industries
- Key takeaways

2 Confidence score and CISO focus

- Confidence challenge: Inhouse expertise, prevention, response and recovery
- Key takeaways

3 Strategic priorities, investments and outsourcing

- Key investment areas
- Outsourcing trends
- Key takeaways

4 Emerging technologies impacting the future

- AI and GenAI
- Automation and IAM
- Key takeaways

Global Cybersecurity Overview

Experienced a cyberattack

57%

of security leaders said their organization experienced a cyberattack in the last 12 months

Anticipating a cyberattack

81%

surveyed highlighted the likelihood of a cyberattack on their organization in the next 12 months

Ability to prevent an attack

48%

indicated their organization has the desired capability to prevent a cyberattack

Difficulty in resuming operations

76%

of security leaders said their organization experienced high to moderate difficulty in resuming operations after the cyberattack

Inhouse expertise

35%

of security leaders indicated they have adequate or more than adequate inhouse security expertise to deal with cybersecurity risks

Global Cybersecurity Overview

Ability to contain, respond and recover

46%

indicated their organization has the desired capability to contain, respond to and recover from a cyberattack

Average budget increase

11%

is the expected average increase in cybersecurity budgets for organizations in 2025

Communication with the board

37%

of security leaders said that they were effective in communicating the state of their IT security posture to the C-suite and the board

Cybersecurity budget

63%

indicated an increase in their organization's cybersecurity budget in 2025

Outsourcing to an MSSP

90%

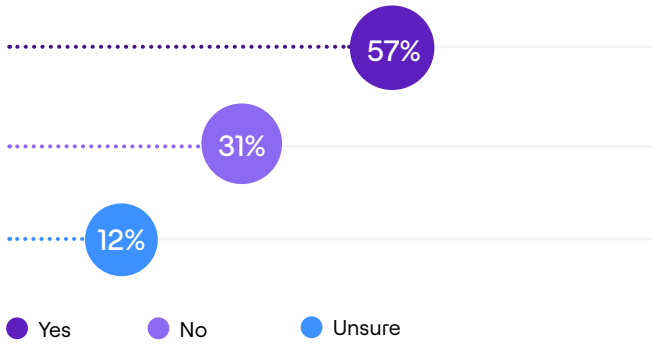
of security leaders said they are outsourcing IT security activities to an MSSP

The new normal of acceptance: Target is everyone

Attack economy: Attacks growing in reach, volume and frequency

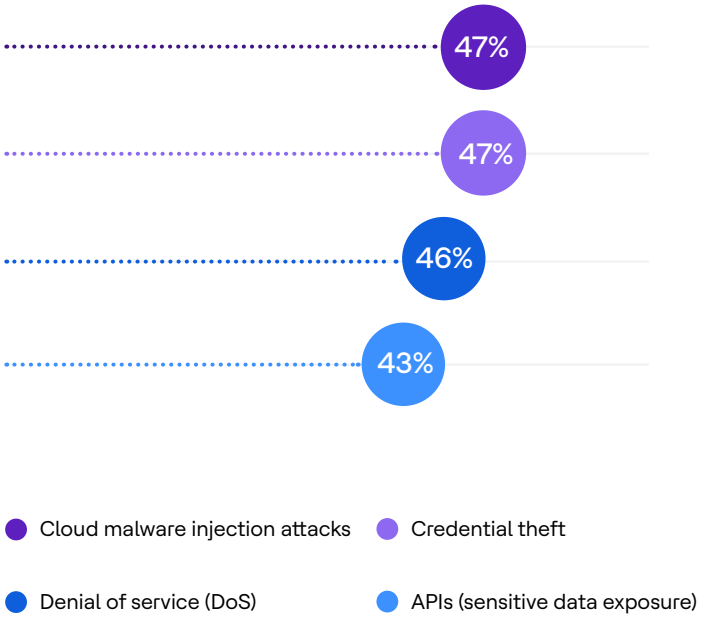
Cyberattacks in the last 12 months

In the past 12 months, 57% of security leaders reported that their organizations faced a cyberattack, while fewer than one-third confirmed no incidents. The growing attack economy continues to evolve, with cyber threats becoming more sophisticated in both reach and volume and threat actors becoming organized crime units, including state funded in many cases. The speed, frequency and impact of these attacks are steadily increasing, posing a significant challenge to organizations across industries. Compounding the issue, many organizations fail to realize they've been breached until almost a year after the attack has occurred. In many cases, it takes months for a breach to be discovered. This latency in detection means the actual number of cyberattacks is likely much higher than what is being reported. As threat actors become more advanced in evading detection, organizations are struggling to keep up, making early detection and timely response critical.



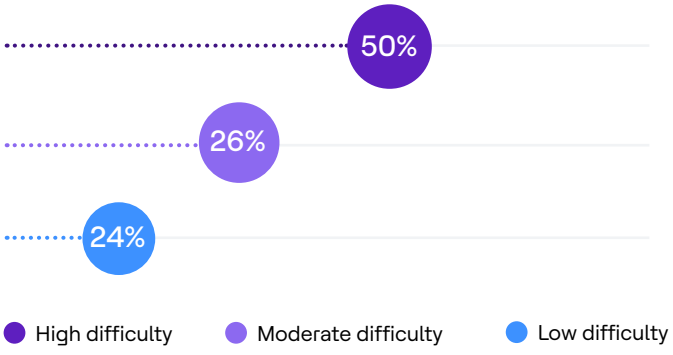
Root cause/attack type used by cybercriminals

Cloud malware injections (47%), credential theft (47%) and API vulnerabilities (46%) were among the methods attackers used to compromise these organizations in the last 12 months. In the case of API vulnerabilities and cloud malware, attackers can use these weaknesses to gain unauthorized access, deploy malware or steal sensitive data. The combination of cloud complexity and API interconnectivity creates more opportunities for these attacks. Credential theft remains a significant threat, where attackers steal login information to gain unauthorized access to systems. This often occurs through AI generated phishing or vishing, social engineering or exploiting weak password policies.



Difficulty in resuming operations

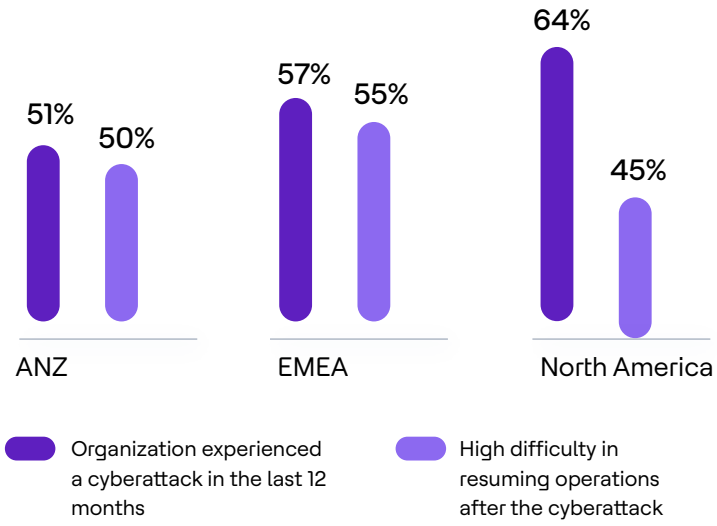
The aftermath was challenging—over three-quarters (76%) admitted they faced moderate to high difficulty resuming normal operations following the attacks. It's no longer a question of if an organization will be attacked, but when. As cyber threats become increasingly sophisticated, organizations must not only focus on preventing attacks but also protecting the backups to enable swift recovery of the crown jewel applications to minimize business disruption. Being able to restore normal operations quickly and efficiently, without hampering business performance, is critical for ensuring long-term operational stability, brand reputation and regulatory penalties in today's dynamic cybersecurity landscape.



Cyberattacks surge in North America and recovery challenges persist in Healthcare

The geo-wise trend of cyberattacks and recovery

North America experienced the brunt of cyberattacks, with 64% of security leaders confirming that their companies were targeted. In EMEA, 57% reported similar incidents, while 51% in ANZ faced attacks. EMEA had the most challenging time bouncing back, with 55% struggling to resume operations after an attack. This global trend emphasizes the importance of building stronger resilience mechanisms across all sectors, with a focus on 24x7 detection, response and recovery to reduce downtime and ensure minimal business disruption. Organizations in these regions must prioritize higher investments in improving their incident response planning and automation to mitigate the growing risks and improve security posture. With global conflicts in play, organizations will need to be extra vigilant towards cyber countermeasures from adversaries in terms of wide scale cyberattacks where many exposed third-party software vulnerabilities could lead to a "collateral damage" situation for many.

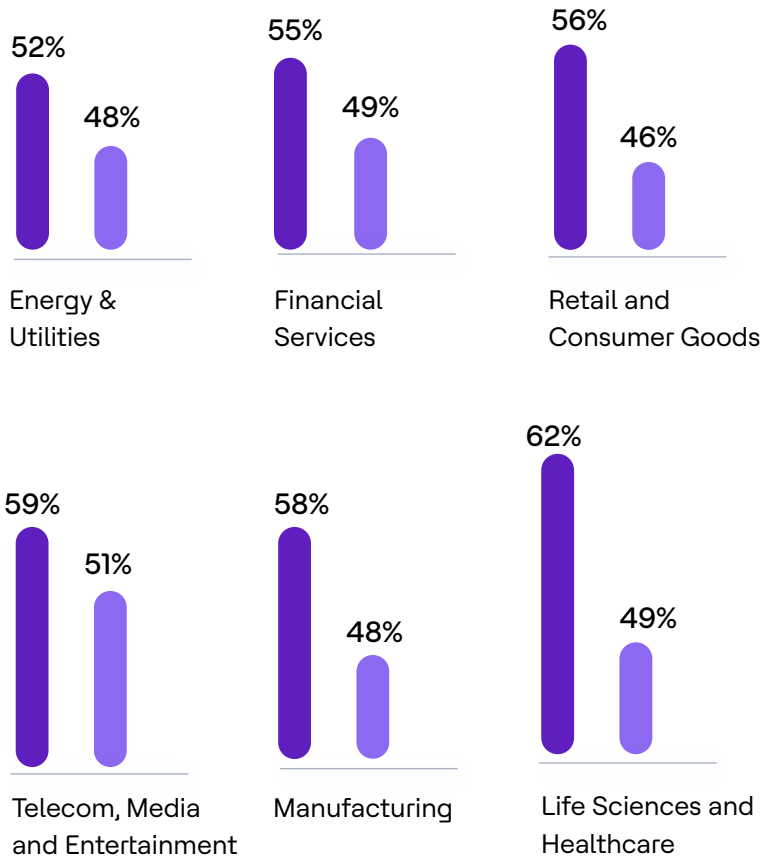


The industry-wise trend of cyberattacks and recovery

Life Sciences and Healthcare took the most brutal hit, with 62% reporting attacks, followed by Telecom, Media and Entertainment (TME) at 59% and Manufacturing at 58%. Security leaders in TME particularly struggled to recover after a cyberattack. Life Sciences and Healthcare struggle with the immediate impact on patient care, TME must contend with disruptions to highly visible citizen services and Manufacturing grapples with production halts and supply chain impacts. Despite the differences, all these industries share a growing need for strong cybersecurity strategies across IT and OT landscapes. These strategies should not only prevent attacks or minimize impact but also enable fast and efficient recovery to minimize disruption and financial impact.

Organization experienced a cyberattack in the last 12 months

High difficulty in resuming operations after the cyberattack



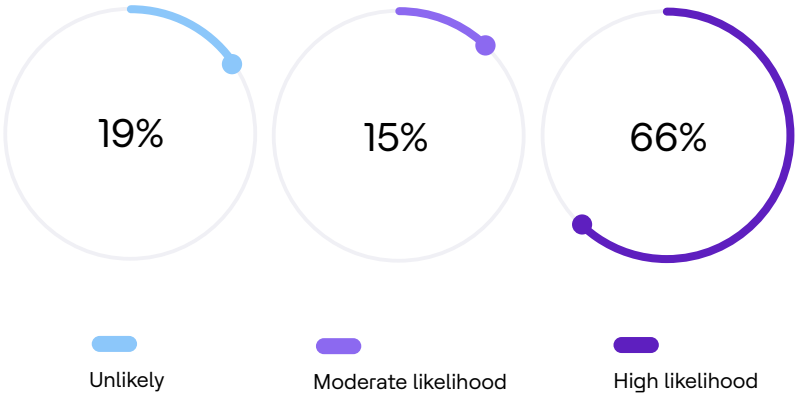
> Cybersecurity has become even more critical as the EMEA region grapples with political and economic challenges. Organizations must take a strategic approach, aligning incident response with business continuity and consolidating security tools. Investing in automation, identity-first security and AI-driven threat detection from trusted MSSPs ensures resilience, compliance and the ability to navigate an increasingly complex cyber and regulatory landscape.

Ashish Kumar Gupta,
Chief Growth Officer,
Europe and Africa,
Diversified Industries,
HCLTech

Top concerns across industries

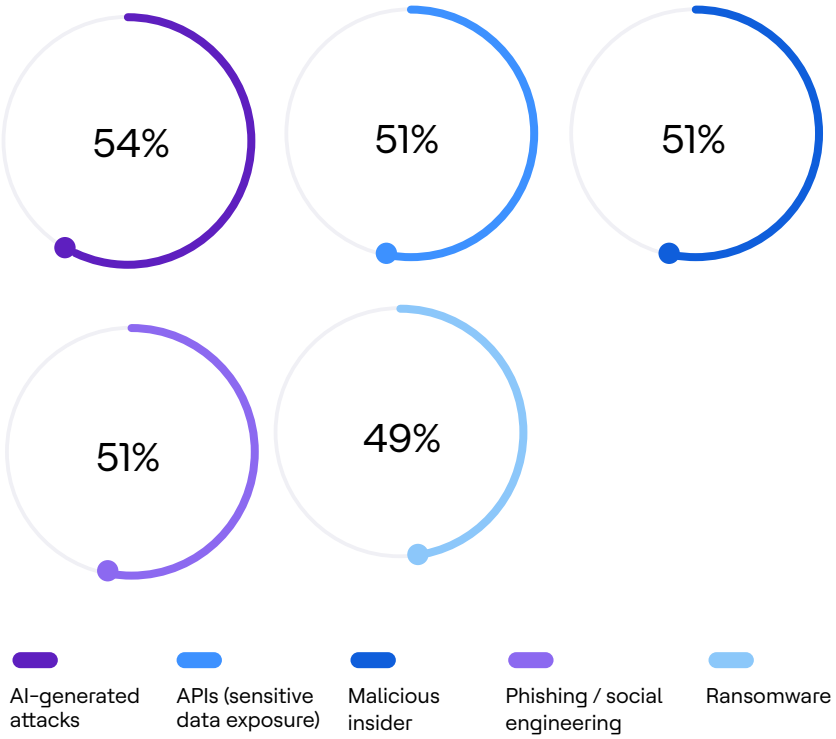
81% of leaders say a cyberattack is likely within the next 12 months

Looking ahead, 81% of security leaders believe there's a moderate to high chance their organization will face a cyberattack in the next year. Geopolitical conflicts are spilling over into the digital realm, with nation-state actors using cyberattacks as tools of disruption, spying and influence. As governments around the world face military tensions, industries—especially critical infrastructure, financial services and healthcare—are becoming prime targets for cyber espionage and sabotage. In the next few months, elections in several major economies will further exacerbate the cyber threat landscape. Elections often lead to a surge in politically motivated cyberattacks, including disinformation campaigns, deep fakes, phishing attacks and targeted disruptions of key systems. These attacks are not limited to government institutions; they frequently extend to industries that provide critical services, such as telecommunications, media and financial services.



AI-generated attacks are now a top concern for CISOs

AI-generated attacks top the list of worries, with 54% most concerned about this emerging threat, followed closely by the risks of phishing, social engineering and malicious insiders. The reason is that malicious actors have increasingly turned to AI to analyze and refine their attack strategies, significantly increasing the likelihood of executing successful phishing/social engineering and ransomware attacks. To secure their organizations, over the next one to two years, organizations must prioritize raising awareness about these AI-enabled cyber threats and fortifying their defenses accordingly.



"In the life sciences and healthcare sector, the rapid adoption of advanced technologies presents both opportunities and cybersecurity risks. It is crucial for CISOs to strengthen recovery strategies through AI-driven SOCs and automated threat response. Addressing gaps in preparedness requires investing in robust training, adopting technologies like Zero Trust and leveraging MSSPs for full spectrum of services. Consolidating security products into integrated platforms can streamline defenses, reduce complexity and enhance overall resilience against evolving threats."

Shrikanth Shetty,
Chief Growth Officer,
Global, Life Sciences and
Healthcare Industries,
HCLTech

AI attacks, API risks and phishing are now top concerns for CISOs

Industries brace for API risks, AI threats and ransomware

Different industries are facing distinct cybersecurity challenges as attack methods evolve. In Manufacturing, 58% of security leaders worry about AI-generated attacks that could disrupt essential production operations, threatening the industry's resilience. For Life Sciences and Healthcare, where sensitive data is at stake, ransomware is the top concern to the PII and PHI data, with 60% viewing it as the biggest threat. In Financial Services, API vulnerabilities are a major worry for 56%, as these can lead to significant data breaches or outages. Retail and Consumer Goods are focused on the risk of malicious insiders (55%), while TME are most concerned about API security (60%). In Energy & Utilities, the fear of AI attacks (60%) is compounded by the risk of malicious insiders (52%), highlighting the need for robust resilience as these threats evolve.

Industry	Top 3 attack vectors security leaders are most concerned about		
	1	2	3
Financial Services	APIs (sensitive data exposure) (56%)	Phishing / social engineering (55%)	AI-generated attacks (53%)
Life Sciences and Healthcare	Ransomware (60%)	APIs (sensitive data exposure) (56%)	Phishing / social engineering (55%)
Manufacturing	AI-generated attacks (58%)	Denial of service (53%)	Phishing / social engineering (51%)
Retail and Consumer Goods	Malicious insider (55%)	APIs (sensitive data exposure) (55%)	Ransomware (52%)
Telecom, Media and Entertainment	APIs (sensitive data exposure) (60%)	Ransomware (58%)	Phishing / social engineering (54%)
Energy & Utilities	AI-generated attacks (60%)	Malicious insider (52%)	Phishing / social engineering (52%)

Key takeaways

Building resilience against AI threats

As AI-generated attacks become a growing threat, organizations need to prepare proactively. Security leaders should simulate real-world scenarios where AI could be weaponized, such as AI-generated phishing emails or adaptive malware. These simulations help identify human or system vulnerabilities and ensure teams are prepared to act swiftly when AI-driven threats materialize. Additionally, investing in organization-wide readiness exercises that engage all departments is important. AI isn't just a threat but also a powerful tool for defenders—who can integrate AI tools or utilities to enhance defenses, automating threat detection and response. By adopting these strategies, CISOs can defend against AI attacks, build resilience and stay ahead of evolving challenges.

Build stronger business alignment and show results

CISOs must focus on aligning cybersecurity strategies with overall business objectives to bridge the gap between IT and business teams. Implementing security measures is not enough; you must communicate how these investments drive reduced risk, improve trust or productivity, revenue acceleration and overall business success. Showcase the quantified risks or tangible results of your efforts, such as threats you've mitigated and improvements in operational efficiency. By demonstrating how your cybersecurity initiatives support business goals, you reinforce the value of these investments and build a stronger case for future funding. This approach reassures the board of your team's impact and enhances organizational resilience against evolving threats.

Focus on resilience and recovery planning across multiple threat vectors

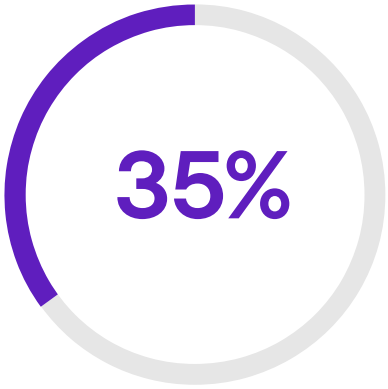
Since 76% of security leaders faced significant challenges resuming operations after attacks, CISOs must enhance their incident response and recovery strategies. Prioritize developing robust resilience strategies tailored to your industry's specific threats—whether it's safe data recovery from ransomware for Life Sciences and Healthcare, stopping AI-generated attacks in Manufacturing or DevSecOps or privilege access to mitigate API vulnerabilities in Financial Services and Telecom. Implement comprehensive data protection and automated recovery tools and procedures. Additionally, conduct regular drills to ensure your organization can quickly and effectively return to normal operations in case of a breach, minimizing downtime and impact.

Confidence score and CISO focus

Confidence challenge: Inhouse expertise, prevention, response and recovery

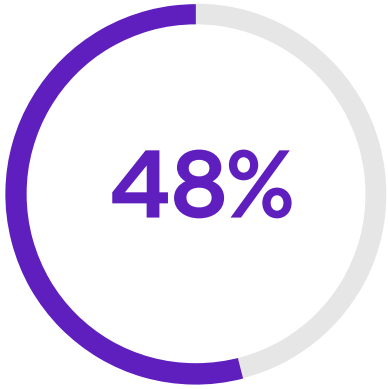
Inhouse expertise

Globally, a mere 35% of security leaders say they have adequate or more than adequate inhouse expertise to deal with security risks and threats facing the organization. This number drops to 30% in EMEA and 34% in North America, though it's higher in ANZ at 42%. This statistic reflects a broader challenge facing organizations worldwide: a significant gap in cybersecurity talent. The shortage of skilled security professionals is exacerbating the inability of organizations to effectively defend against sophisticated attacks. The low confidence scores across regions highlight a pressing need for upskilling internal teams and investing in cybersecurity talent development. In addition, organizations must confidently leverage external partners for sourcing strategic capabilities like detection and response, Cyber assurance, technology lifecycle management and governance of risks and compliance.



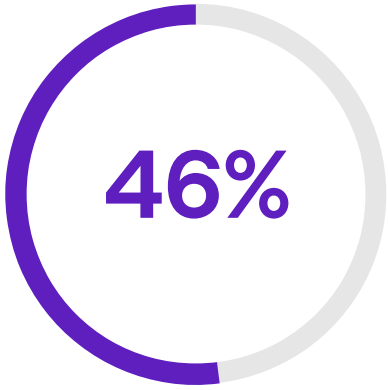
Preventing an attack

Globally, only 48% indicated that their organization can prevent a cyberattack. This suggests a significant gap in preparedness, as 81% anticipate a high likelihood of a cyberattack. EMEA leads with 58% confidence, followed by North America at 47%. ANZ lags at 40%. This gap in preparedness is not just a technical issue but also a leadership challenge. Security leaders must focus on improving communication with the C-suite and board of directors to secure the necessary investments in advanced technologies and skilled personnel. Without significant improvements in both the technical and strategic aspects of cybersecurity, organizations will continue to struggle to keep up with the rapidly evolving threat landscape.



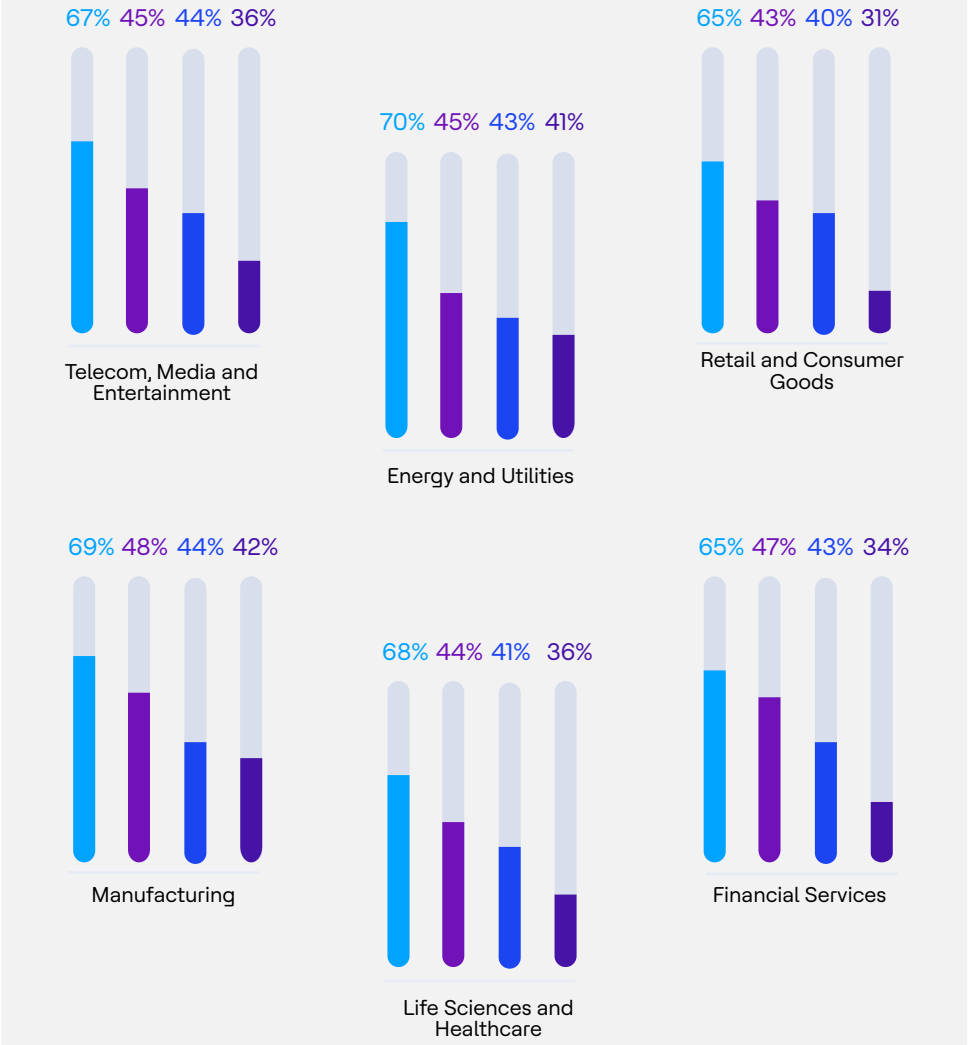
Respond and recover

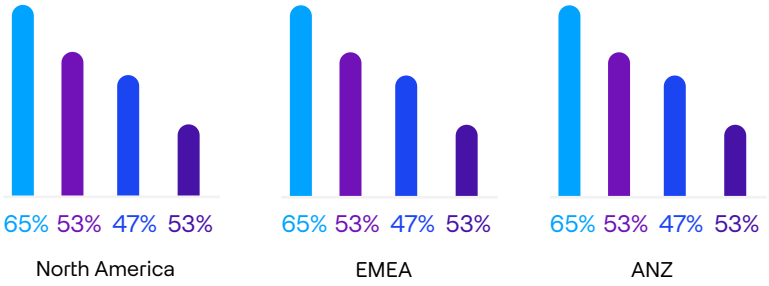
Only 46% indicated that their organization has a high ability to contain, respond to and recover from a cyberattack, indicating a difficulty in improving cybersecurity posture. North America fares better at 53%, but EMEA (40%) and ANZ (43%) are lower. These figures highlight significant gaps in both preparedness and response capabilities across regions. The low confidence score also reflects a broader issue with cybersecurity resilience. While prevention remains a priority, organizations must place equal emphasis on their ability to respond and recover swiftly. Investing in incident response automation, real-time monitoring, business continuity and disaster recovery planning, including cyber drills, will be critical in closing these gaps.



Gaps in expertise, prevention and response across regions and industries

Financial Services (65%) and Life Sciences and Healthcare (68%) face a high likelihood of cyberattacks. These sectors show varying levels of inhouse expertise and prevention strategies. Manufacturing leads with the highest perceived inhouse expertise at 48% and slightly more robust perceived recovery capabilities at 42%. Retail and Consumer Goods and Telecom, Media and Entertainment have moderate confidence in handling cyber threats. However, a significant concern is the low percentage of organizations with solid prevention and response capabilities. Only about one-third of organizations feel equipped to prevent and respond to cyberattacks, meaning that around two-thirds are not fully prepared to tackle these threats effectively. This highlights a widespread gap in cybersecurity readiness across industries and – on top of concerns related to effectiveness of board of directors communication – points to a gravity of the challenge that needs to be addressed.





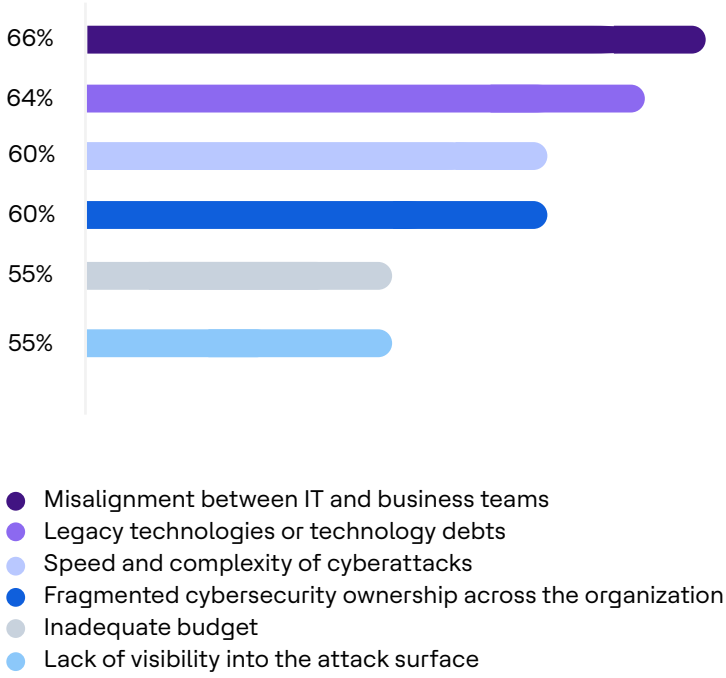
- High likelihood of cyberattack in the next 12 months
- Inhouse IT security expertise (adequate or more than adequate)
- Ability to prevent a cyberattack
- Ability to contain, respond and recover from a cyberattack

CISO focus: Key barriers to cybersecurity effectiveness

Pain points in addressing the changing threat landscape

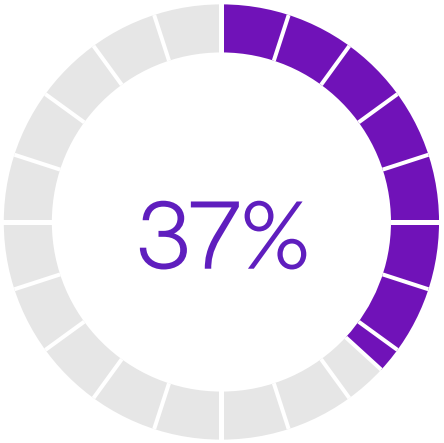
Misalignment between IT and business teams hinders cybersecurity leaders from achieving full effectiveness of executed strategies and overall cyber resilience, according to 66% of security leaders. Contributing to this issue is that only 37% rate their effectiveness in communicating the state of their IT security posture to senior management and the board of directors as very or highly effective.

Other serious challenges include legacy technologies or technology debt (64%), fragmented cybersecurity ownership across the organization (60%), speed and complexity of cyberattacks (60%), inadequate budget (55%) and lack of visibility into the attack surface (55%).



Effectiveness in communicating the state of the IT security posture to senior management and the board of directors

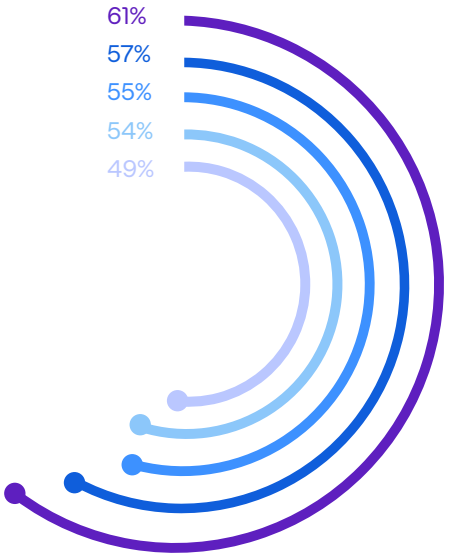
Only 37% indicated they effectively communicated the state of their IT security posture to senior management and the board of directors. Security leaders who can effectively communicate the business value of their efforts will be better positioned to secure the necessary funding and executive buy-in to strengthen their organization's cybersecurity posture. This involves not just highlighting risks but also quantifying their impact and showcasing the return on investment (ROI) of past security initiatives, whether it's through improved incident response times, reduced downtime or enhanced compliance with regulatory standards.



CISO focus: Cybersecurity leaders focus on governance and compliance, face challenges in communication and insurance coverage

Key governance practices for IT security leaders in the next 1-2 years

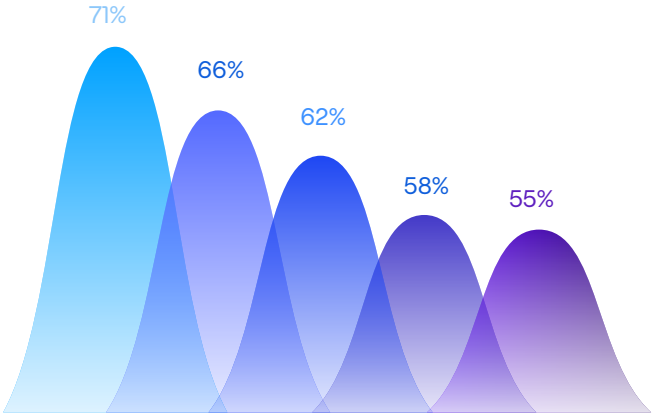
Effective communication about cybersecurity threats and successes is crucial: 61% of leaders say frequent updates to C-level executives and boards are essential, with 55% emphasizing reporting on the effectiveness of IT security in reducing breaches and 54% focused on maintaining inhouse expertise. Over the next two years, aligning IT security with business strategy, maintaining a skilled inhouse team and fostering a security-conscious culture will be essential governance practices that define how organizations defend against and recover from the ever-growing cyber threats.



- Frequent communication to C-level executives and board members about the threats against the organization
- Conduct regular risk assessments and incorporate them in our organization's cybersecurity strategy
- Frequent communications about the effectiveness of IT and the IT security functions in reducing data breaches and other security incidents
- Ability to maintain and retain inhouse cybersecurity
- Creation of an innovative and agile IT security function

Top 5 cybersecurity tasks taking up security leaders' time

Security leaders report spending the majority of their time focused on several key activities, with many indicating they balance efforts across multiple areas. Leaders say they dedicate significant time to cyber program governance for ensuring ROI (71%), ensuring compliance with new privacy and security regulations (66%) and responding to security incidents (62%). These tasks are essential in maintaining organizational resilience and meeting regulatory requirements in an increasingly complex cybersecurity landscape.



- Cyber program governance
- Cybersecurity strategy and roadmap
- Responding to security incidents
- Management briefings and education
- Compliance with privacy and regulations

Key takeaways

Enhance inhouse expertise, talent retention and strategic partnerships

With only 35% of global security leaders confident in their inhouse expertise, and even lower confidence in EMEA and North America, it's clear that skill gaps are a significant concern. To address this, focus on investing in targeted training for your team and consider bringing in consultants and specialized service providers. These experts can offer advanced knowledge and tools that your team might lack, helping you stay ahead of complex threats. Regularly engage with these consultants to update your team on the latest security practices and technologies and targeted threat intelligence. Combining internal skill-building with external expertise will fill critical gaps, enhance security posture and boost your organization's resilience. This holistic approach will better prepare your team to effectively handle evolving cyber threats.

Prepare, test, learn

With less than half of security leaders confident in their organization's ability to respond to and recover from a cyberattack, enhancing your incident response plan for greater resilience is crucial. Build a dynamic response framework, run regular drills and ensure quick access to external recovery support. At the same time, since only 48% believe their organization can prevent attacks effectively, invest in advanced threat detection tools and perform regular vulnerability assessments. Simulate attacks to identify and address weaknesses. This is especially important in regions like ANZ and North America, where confidence in prevention is lower. Strengthening your prevention strategies and response capabilities will improve your organization's resilience against evolving threats.

Communicate effectively and prioritize governance

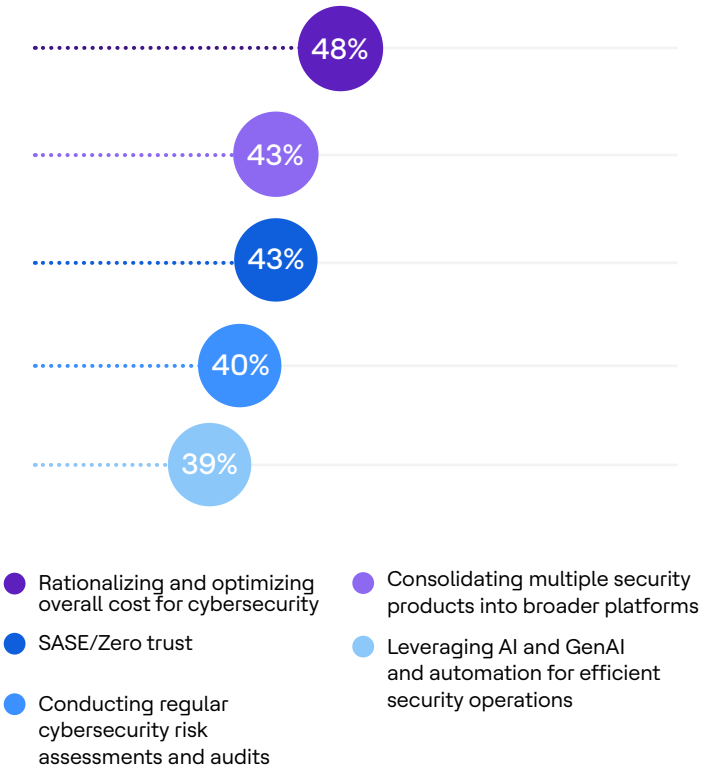
Effective communication about cybersecurity threats and successes is crucial, but only 37% of leaders feel they excel in this area. CISOs should focus on presenting clear, concise risk program updates tailored to the board and C-suite to bridge this gap. Use business (non-technical) language and highlight key metrics that demonstrate the impact or progress of cybersecurity efforts on business objectives. Regularly share updates on resilience measures, potential risks and how investments in security align with organizational goals. Additionally, with nearly 27% of organizations in the process of acquiring additional insurance or coverage expansion, ensure your board understands the importance of this coverage. Cyber insurance can provide crucial protection against breaches and mitigate financial impacts. Improving communication and securing adequate insurance will strengthen your organization's cybersecurity posture and resilience.

Strategic priorities, investments and external sourcing

Prioritizing IT security infrastructure, cost efficiency and compliance for a more robust cybersecurity posture

Top strategic priorities for cybersecurity in the next 1-2 years

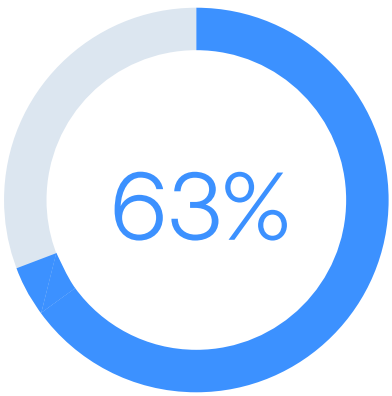
As organizations face mounting financial pressures and an increasingly complex cyber threat landscape, reducing waste and ensuring smart spending in cybersecurity is critical. Rationalizing and optimizing the overall cost for cybersecurity (48%) is the top strategic priority for security leaders. Other priorities are consolidating multiple security products into broader platforms (43%) and implementing Zero Trust and a SASE (secure access service edge) architecture that combines networking and security as a service function into a single cloud-delivered service at the network edge (43%). Security leaders must carefully balance cost efficiency with operational effectiveness, ensuring that every investment directly contributes to a more resilient and agile cybersecurity posture. By focusing on consolidation, automation and continuous risk assessment, organizations can build a cost-effective and scalable security framework that meets both current and future challenges.



Security leaders plan to boost cyber budgets by 11% in 2025

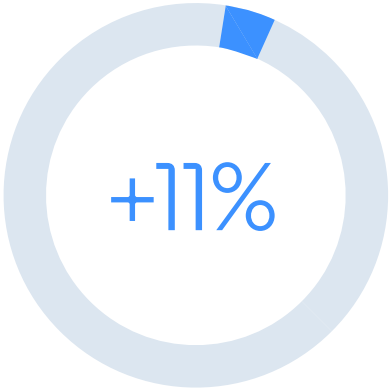
Planning to increase budget

A notable 63% of security leaders have indicated that their organizations plan to increase cybersecurity budgets in 2025, signaling not just a response to past incidents but a forward-looking approach to counter future threats, particularly AI-driven attacks and evolving malware. This surge in budget allocation reflects a broader shift in how organizations view cybersecurity. No longer seen as a mere technical safeguard, cybersecurity is now understood as a business enabler, essential for protecting digital transformation initiatives, maintaining customer trust and ensuring business continuity. In some of the industries included in the survey, this increased investment may need to be funded from broader IT budgets (self-funding initiatives).



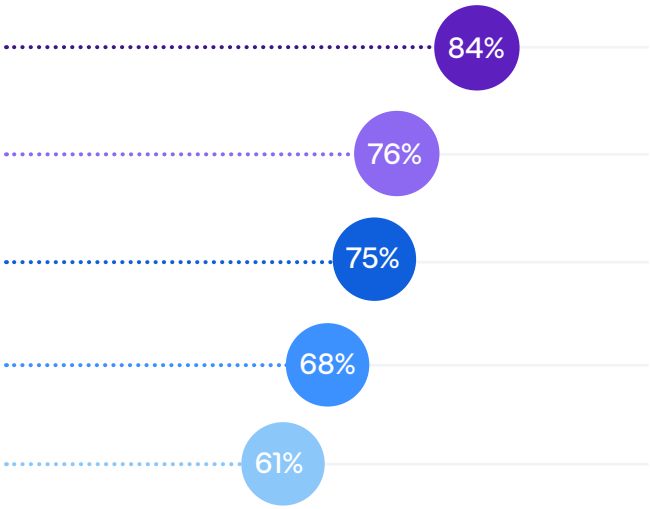
Average increase in budget

In 2025, companies are expected to raise their cybersecurity budgets by an average of 11%. This is more than just a number—it reflects a proactive approach by businesses to protect themselves from the immediate dangers and build a stronger, more resilient foundation for the future. This additional funding opens opportunities for businesses to explore cutting-edge technologies like AI-driven threat detection, security automation and Zero Trust frameworks, IoT/IIoT security and 5G security — increasingly necessary tools in today's fast-paced digital world.



Key cybersecurity budget investments for the next 1-2 years

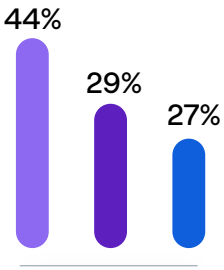
In the next one to two years, the primary goals of cybersecurity budgets are to improve compliance and move to real-time risk management, with security leaders predicting an average budget increase of 11%. Investment priorities include improving compliance and risk management (84%), SOC automation (76%), incident response and recovery (75%), incident response plans (68%), practices to achieve cyber resilience (61%) and threat intelligence (68%).



- Improving compliance, risk management
- SOC automation
- Incident response and recovery
- Threat intelligence
- Practices to achieve cyber resilience

Plans for cyber insurance

In an era when cyberattacks are growing in frequency and sophistication, cyber insurance provides an essential defense against the financial and operational impacts of cyberattacks. Nearly 27% of security leaders said their the organization plans to purchase additional cybersecurity insurance or increase the existing coverage while 73% believe they can't get any bigger safety net or risk tradeoff through insurance and have no plans to buy additional coverages.



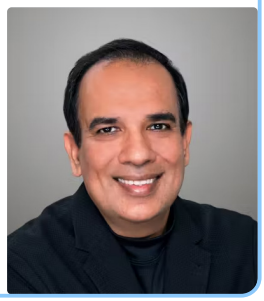
- Our organization has cybersecurity insurance
- We have no plans to purchase additional cybersecurity insurance
- Our organization is in the process of purchasing cybersecurity insurance

> In the financial services sector, balancing evolving regulations with robust data protection is crucial. As firms undergo digital transformation, they face heightened cyber threats and regulatory challenges. Adopting advanced solutions like Zero Trust, AI and SOC automation is essential. Partnering with MSSPs provides necessary expertise, while AI and automation enhance recovery and minimize disruptions. A flexible, comprehensive cybersecurity framework is key to managing threats and ensuring operational security."

Srinivasan Seshadri,
Chief Growth Officer and Global Head, Financial Services, HCLTech

In the face of increasing supply chain attacks and evolving threats targeting operational technology (OT) environments, strengthening post-attack recovery is crucial. AI-driven Security Operations Centers (SOCs) play a vital role in automating threat detection and incident response, which is essential for rapidly containing ransomware and credential theft. Regular disaster recovery drills and updated response playbooks are necessary to prepare for real-world scenarios. Investing in advanced technologies such as Managed Detection and Response systems protects critical data. It supports business continuity, ensuring that operations can resume swiftly and securely after an incident."

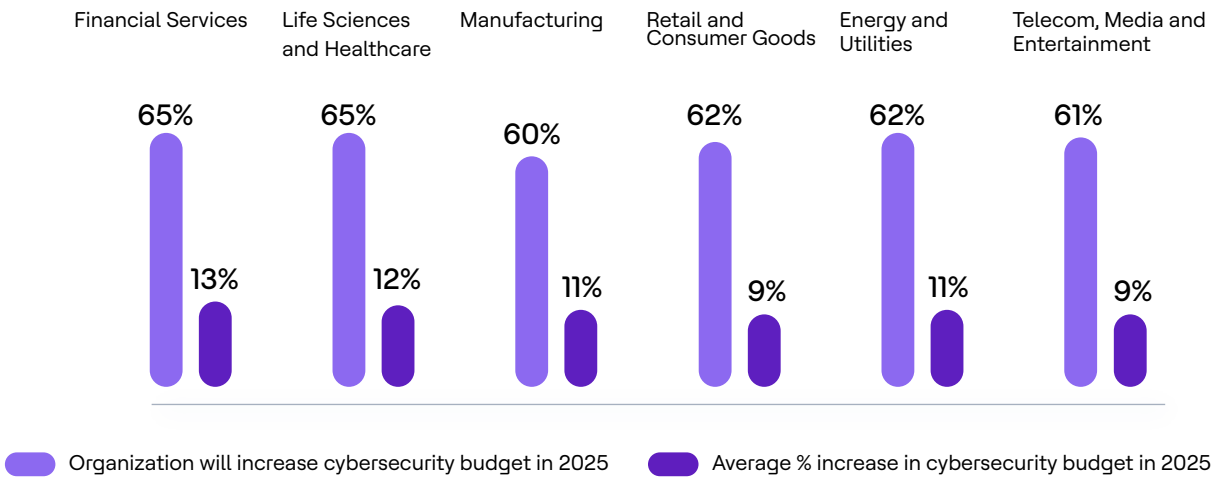
Ajay Bahl
Chief Growth Officer,
Americas, Mega Industries,
HCLTech



Security budgets set to grow in 2025: North America leads with 13% increase

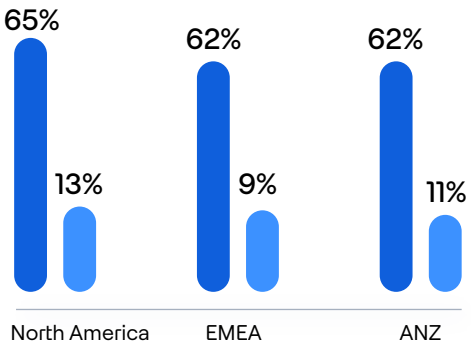
Cybersecurity budget increase in 2025 by industry

As we look to 2025, many industries prioritize cybersecurity with planned budget increases. Financial Services and Life Sciences and Healthcare are leading the way, with 65% of organizations aiming to boost their budgets by 11%. Manufacturing and Energy and Utilities aren't far behind, with 60%-62% of organizations setting aside an 11% increase. Whether it's protecting financial transactions, ensuring the safety of healthcare data or maintaining the flow of energy and manufacturing, organizations recognize that cybersecurity is no longer optional—it's an essential pillar of business continuity, regulatory compliance and customer trust.



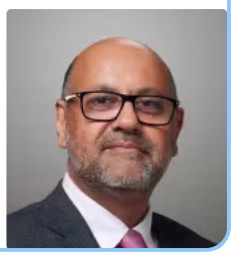
Cybersecurity budget increase in 2025 by region

In North America, 65% of leaders are pushing for an average increase of 13%, underscoring a solid commitment to fortify defenses. In EMEA, 62% aim for a 9% boost and ANZ is targeting an 11% rise, with 62% of leaders on board. This growing investment reflects a heightened focus on tackling emerging cyber threats and strengthening security strategies.



Cybersecurity is at the heart of enabling the Telecom, Media and Entertainment industry to supercharge progress in an era of digital transformation. As AI and automation expand capabilities, the attack surface becomes more complex. Security must shift from being a reactive measure to a strategic enabler that protects the total experience—across customer, employee and partner interactions. For businesses, securing seamless and personalized experiences is essential not just for protection but for maintaining trust, promote innovation and staying competitive in an evolving landscape."

Anil Ganjoo,
Chief Growth Officer – Americas, RCPG and TMT Industries, HCLTech



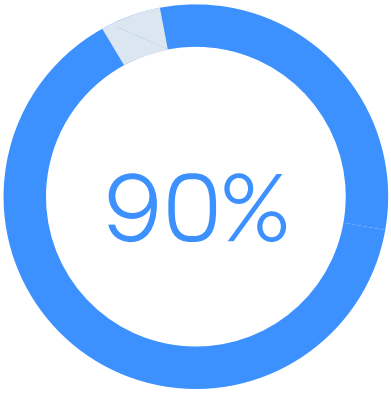
As the threat landscape intensifies, the HCLTech report highlights the shift in focus among security leaders from flashy trends to essential measures. CISOs worldwide must prioritize establishing strong defense mechanisms and recovery strategies against potential attacks. Additionally, they should drive efficient and effective cybersecurity outcomes by leveraging automation and strategically consolidating tools through platformization. This proactive approach will ensure the security of organizations as they undergo digital transformations, which expand attack surfaces and face increasingly sophisticated attacks driven by AI innovations."

Anand Oswal,
SVP and GM, Network Security, Palo Alto Networks

Rising budgets and outsourcing: Security leaders eye MSSP partnerships

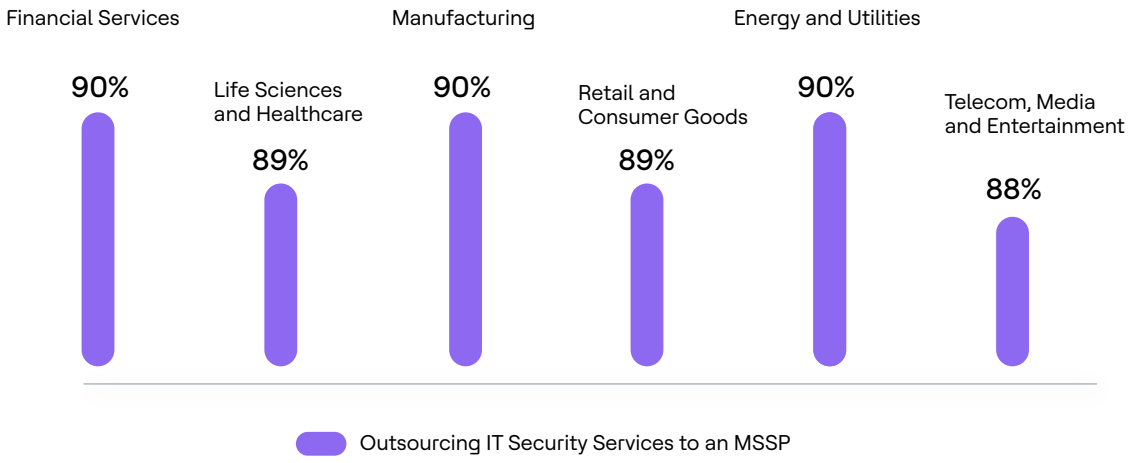
Outsourcing

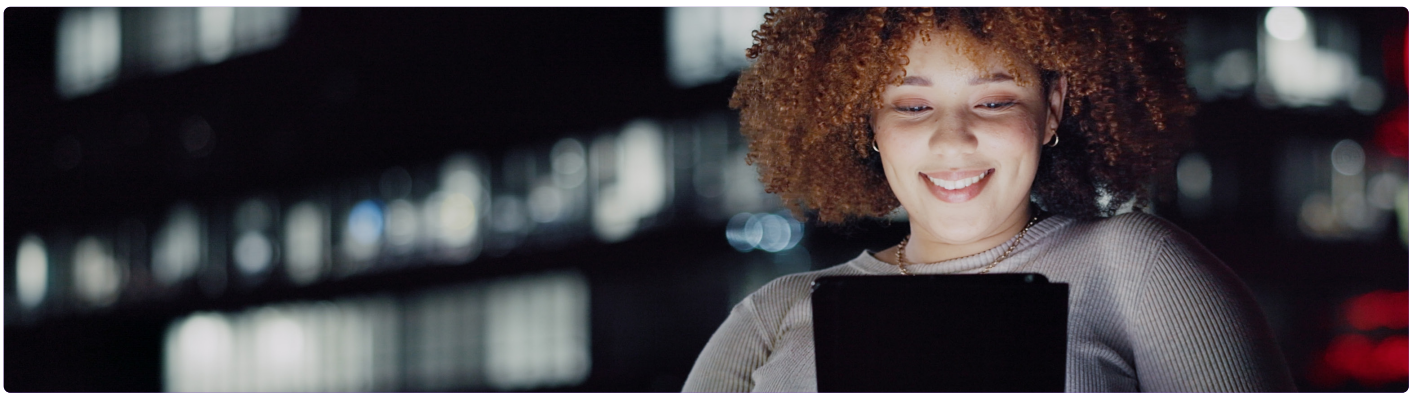
A huge majority of organizations (90%) turn to Managed Security Service Providers (MSSPs) to outsource key IT security activities. This widespread shift toward outsourcing highlights an essential trend in the industry: businesses are recognizing that they often lack the inhouse expertise, resources or bandwidth to effectively manage all aspects of cybersecurity on their own.



Outsourcing work to MSSPs by industry

Around 90% of security leaders in sectors like Financial Services, Manufacturing and Energy and Utilities now rely on MSSPs to handle some of their cybersecurity efforts. The increasing reliance on MSSPs isn't just a cost-saving measure—it reflects the reality that organizations face more sophisticated cyber threats than ever before. In industries like Financial Services, where protecting sensitive customer data is a top priority, MSSPs bring advanced tools and round-the-clock threat monitoring that inhouse teams often struggle to provide. In Manufacturing and Energy and Utilities, the stakes are just as high. With the rise of connected technologies and intelligent systems, these industries face new vulnerabilities in their operational technology (OT). MSSPs help manage and secure these systems, bridging the gap between IT and OT security, which can be difficult for inhouse teams to handle alone.





Key takeaways

Focus on efficiency and free up budgets

It's all about getting more out of your IT security setup in the next year or two. Start by simplifying your security tools—consolidate where you can and look into SASE/Zero Trust to reduce complexity and costs. Nearly half of security leaders are prioritizing cost optimization in cybersecurity. Consider consolidating various security tools into broader, more integrated platforms to make the most of your budget and reduce the complexity of integration and skills needed. Adopting solutions like Secure Access Service Edge (SASE) or a Zero Trust framework can help you combine security and networking into one efficient service. This not only cuts down on complexity but also enhances your security posture. By focusing on cost-effective and integrated solutions, you'll streamline operations and be better prepared to handle emerging threats.

Prioritize spend areas and choose the right partner

Focus your investments on areas that matter most—like threat intelligence and incident response. With most organizations leaning on MSSPs for support, choose partners who excel in security capabilities, have a global reach and have a proven track record. Ensure your partnerships are genuinely delivering the value and security your organization needs. Outsourcing tasks like threat detection and incident response can fill gaps in your inhouse expertise and provide around-the-clock protection. This partnership will give you access to advanced tools and specialized skills while allowing your internal team to focus on strategic priorities, ultimately enhancing your organization's security and resilience.

Invest in compliance, automation and building resilience

With cybersecurity budgets set to increase by an average of 11% in 2025, now is the time to invest in areas that will strengthen your security. Prioritize spending on improving real-time risk management and compliance, automating your Security Operations Center (SOC) and enhancing incident response plans. These investments will help you stay on top of regulatory requirements and effectively manage threats. By focusing on automation and resilience, you'll meet compliance goals and build a more robust security framework.

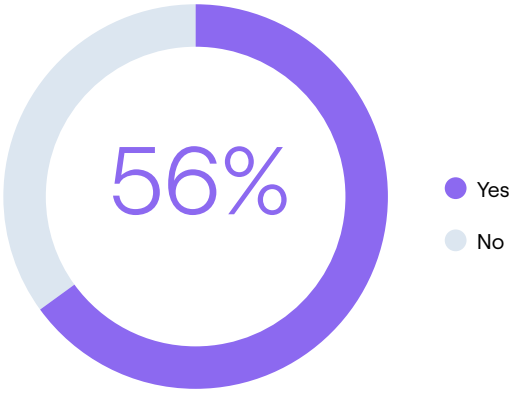
Emerging technologies impacting the future

Cybersecurity automation

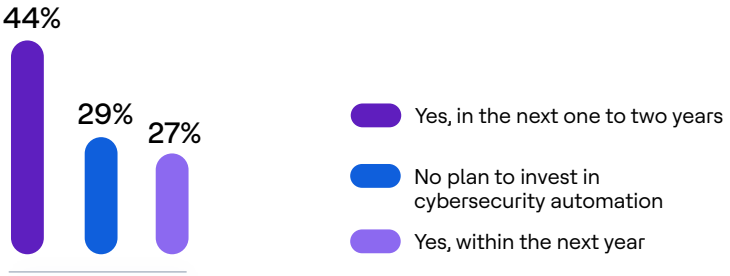
Cyber automation is automatically detecting, investigating and remediating cyber threats—with or without human intervention—using a programmatic solution designed explicitly for that purpose. It works by identifying threats to an organization's security posture, sorting them and performing triage on them. Automation is instrumental in helping streamline the multitude of alerts organizations deal with daily.

Invested in cyber automation

56% of security leaders say their organizations have invested in cybersecurity automation. Of those who haven't (44%), 27% say they will invest in the next year and 44% say they will invest in the next one to two years. Only 29% say they have no plans to further invest in cybersecurity automation.



Plans to invest in cyber automation for the 44% who haven't already done so



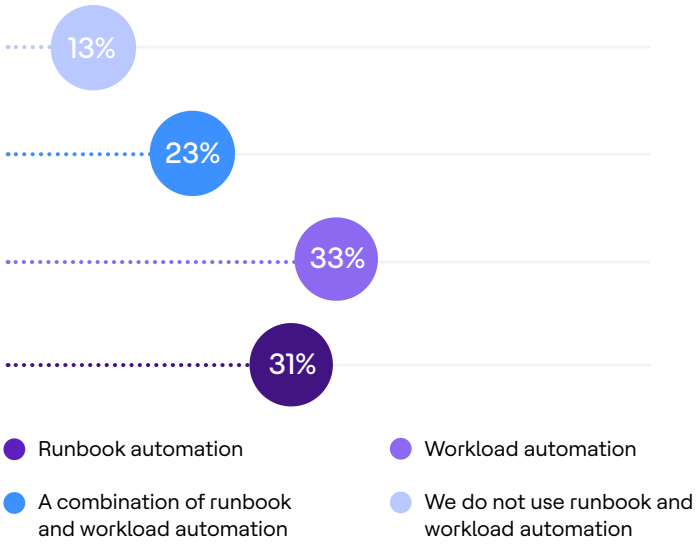
Cybersecurity automation: Cost savings vs. implementation challenges

Top motivators for investing in cybersecurity automation

Reducing costs is the primary reason most organizations have invested in cybersecurity automation. As discussed previously, making the IT security infrastructure more efficient to reduce costs is a strategic priority.

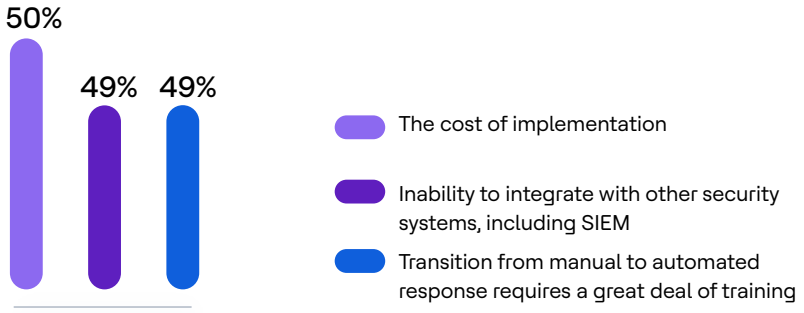
Organization approach to cybersecurity automation

Automation is critical for organizations to streamline workloads and maximize productivity. There are many kinds of automation, and 33% of security leaders say their organization's approach to automation is workload automation. A workload automation solution manages tasks, often called jobs or workloads, across mainframes, distributed servers, containers, applications and clouds. A runbook automation approach (30%) is based on documented operating procedures to complete specific IT tasks and processes. Runbooks provide a scripted method to consistently deploy, start, stop and support systems within an organization. By standardizing procedures, runbooks enable efficiency and consistency, simplify onboarding for new hires and improve knowledge transfers between employees and teams.



Pain points or challenges in using cybersecurity automation

While most organizations plan to invest in cybersecurity automation, its implementation has certain challenges, including the cost of implementation (50%), the inability to integrate with other security systems, including SIEM (49%), and the fact that the transition from manual to automated response requires a great deal of training (49%).

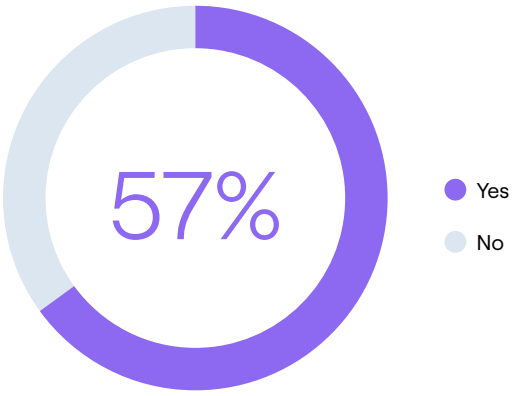


> Reflecting on the evolution of cybersecurity, it's clear that we have come a long way. From the early days of basic antivirus software to today's sophisticated AI-driven security solutions, the security technology landscape has transformed dramatically to meet the rapidly evolving threat landscape. Microsoft processes 78 trillion threat signals each day, and our threat intelligence research indicates that threat actors are not only growing in numbers, but they are collaborating with each other and using AI-based techniques and tactics. I believe that defenders must leverage the superpowers of generative AI to gain an advantage; and at the same time, we need to build AI that is trustworthy. Ultimately, security is a team sport, and we need to work together as an industry to build collective defenses. By doing so, we can build a safer digital world for everyone."

Vasu Jakkal,
CVP, Microsoft Security, Microsoft

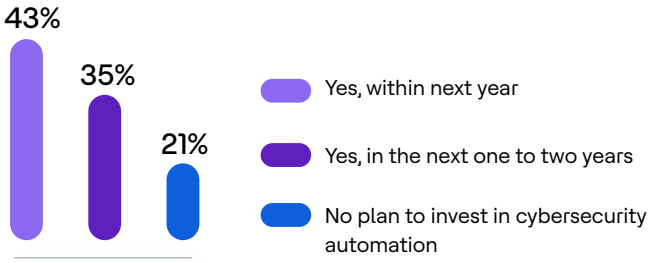
AI and GenAI in cybersecurity

GenAI refers to a category of AI algorithms that generates new outputs based on large language models on which they have been trained. This is unlike machine learning systems designed to recognize patterns and make predictions. Compared to the standard neural network-based generative AI associated with large language models, recent advancements in generative AI further advance threat detection and response capabilities. Dynamic-based generative AI models are better positioned to analyze complex systems, such as network infrastructures or software applications, to identify vulnerabilities, detect novel threats and mitigate risks.



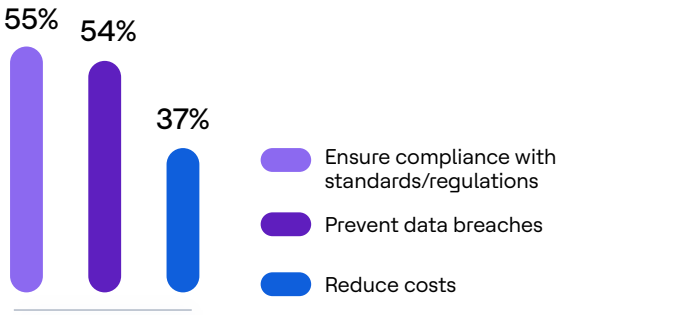
Investments in AI and GenAI for cybersecurity

Organizations recognize that investing in AI and GenAI is the future of reducing the occurrence of cyberattacks. 57% of security leaders say their organizations invested in AI and are exploring GenAI actively. Of the 43% who haven't, 43% say they will invest in AI and GenAI within the next year and 35% in the next one to two years. Only 21% say there is no plan to invest in AI and GenAI. We believe almost everyone will have to use AI/GenAI to defend against AI-based attacks, and while there is still low confidence in GenAI outcomes, many are exploring the same in their operations environments.



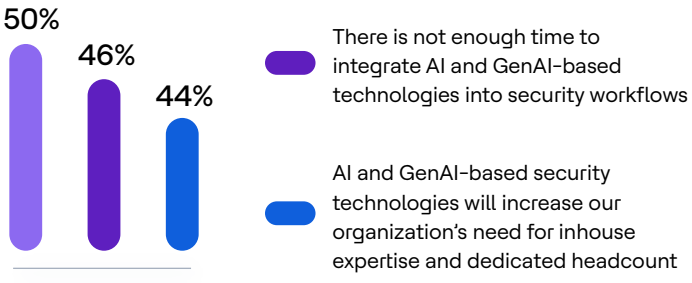
Critical drivers for AI and GenAI investments in cybersecurity

Investments in AI and GenAI are gaining momentum across industries, driven by critical business and security needs. For security leaders, three primary motivators stand out when it comes to embracing these advanced technologies: ensuring compliance with industry standards and regulations (55%), preventing data breaches (54%) and reducing costs (37%). The challenge is to balance these investments with a strong governance framework that ensures both effectiveness and security as they embrace the future of AI-driven cybersecurity.



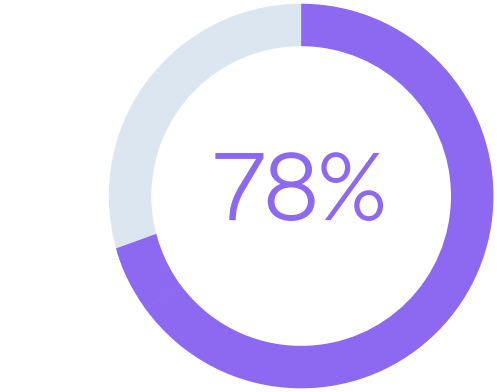
Challenges of using AI and GenAI in cybersecurity

Integrating AI and GenAI into existing cybersecurity frameworks is a significant challenge for many organizations, especially when aligning these advanced technologies with legacy systems (50%) and traditional workflows (46%). The complexity of older infrastructure, often built on outdated technologies, creates roadblocks that make seamless integration daunting. Other concerns are the need for inhouse expertise and a dedicated headcount (44%).



Digital identity: Investments and roadmap

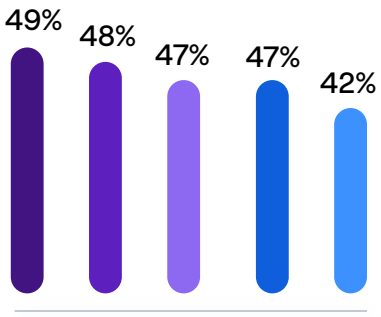
Digital Identity or Identity and Access Management (IAM) technologies focus on defining and managing roles and the associated access privileges of users. Improved user experience and the increase in the number of regulations or industry mandates are the main motivators for investing in IAM technologies. 44% of security leaders say their organizations have invested in advanced modern IAM technologies.



78% of security leaders plan to refresh IAM technologies in the next 1-2 years

Top IAM technologies or activities organizations will invest in the next 1-2 years

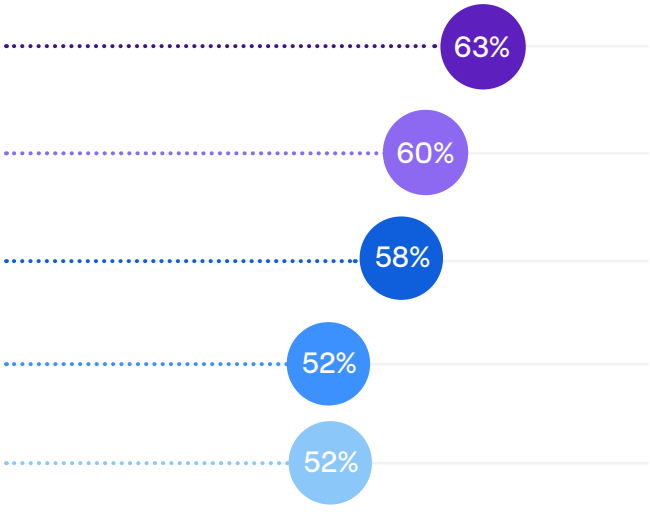
In the next one to two years, the IAM technologies or activities most likely to be invested in are identity governance (49%), customer identity and access management (48%), privileged access management (47%), multifactor authentication and single sign-on (47%) and machine identity and access management (42%).



- Identity governance (IGA)
- Customer identity and access management (CIAM)
- Priviledged access (PAM)
- Machine identity and access management
- Multifactor authentication and single sign on

Top motivators for investing in IAM

The top motivators for investing in IAM technologies include improved user experience (63%), the increase in the number of regulations or industry mandates (60%), constant turnover of employees, contractors, consultants and partners (58%) and to secure privilege access (52%).



- Improved user experience
- The increase in the number of regulations or industry mandates
- The constant turnover of employees, contractors, consultants and partners
- The constant changes to the organization due to corporate reorganizations, downsizing and financial distress
- To secure privilege access

Key takeaways

Streamline your operations with cyber automation

As cyber threats become more frequent and complex, automation can be a game-changer for your team. Look into implementing both workload and runbook automation to handle routine tasks efficiently. Investing in cybersecurity automation can significantly reduce costs and increase efficiency. This will help manage the flood of alerts and free up your team to tackle more pressing security challenges. Ensure your automation tools integrate smoothly with your existing systems to get the most out of them.

Navigate AI and GenAI integration with care

AI and GenAI are exciting tools for enhancing cybersecurity, but integrating them with your current systems can be tricky. Focus on building a solid governance framework to guide the deployment of these technologies. Look at updating any outdated systems and invest in training to help your team adapt. By carefully managing the integration process and addressing these challenges head on, you can harness the power of AI while ensuring your security remains robust and effective.

Strengthen IAM for better security and compliance

As regulatory requirements grow and user management becomes more complex, strong Identity and Access Management (IAM) systems are crucial. Focus on enhancing identity governance, managing privileged access and improving user experience. Investing in IAM technologies will help you stay compliant, secure sensitive data and manage access more effectively, especially as your organization navigates constant personnel changes and evolving access needs. This means viewing identity as the foundation of your cybersecurity strategy, ensuring robust controls and continuous monitoring. Choose IAM solutions that integrate smoothly with your existing systems and support features like real-time access management. By prioritizing identity-first security, you'll enhance your ability to protect sensitive data, streamline access management and maintain compliance, fortifying your overall security posture.

HCLTech

Supercharging Progress™

hcltech.com