CDG | CYBER DEFENSE GROUP

Perception or Reality?
CxO Disconnects Leave Organizations Vulnerable to Security Threats

Despite rising security budgets, perceptions around cyber threats and strategies reveal a critical gap in leadership confidence and readiness.

Contents

Executive Summary

Cyber risks are escalating, forcing a reckoning in the priorities of C-suite leaders across enterprises and mid-sized businesses globally. Executives recognize the need to adapt their strategies and enhance their capabilities to navigate emerging opportunities, such as accelerated innovation and data monetization, and new threats, including those driven by artificial intelligence (AI).

In this context, the Cyber Defense Group releases its first annual security support study, **Perception or reality? CXO disconnects leave organizations vulnerable to security threats.** This independent survey, conducted with 300 industry leaders, seeks to shed light on key business strengths, identify critical concerns, and highlight any misalignments that may be undermining security strategies and execution in today's landscape.

While most executives express confidence in their cybersecurity strategies, the level of confidence varies by role and leadership level. Based on our experience, this confidence is misplaced in many cases. In addition, most organizations are only modestly increasing cybersecurity budgets this year. **Could this indicate a difference between perception and reality?**

Perception versus reality:
90% of leaders believe their cybersecurity strategies are strong, yet nearly half have suffered breaches. This disconnect exposes critical vulnerabilities

Executives know that running and growing a business is significantly more challenging in the age of AI.

- **The attack surface is rapidly expanding:** Companies are digitizing more data, adopting open-source tools to accelerate and productionize AI and machine learning (ML) models, and relying on APIs to link systems and collaborate with third-party vendors. These practices create an increasingly target-rich environment, attracting adversaries seeking to exploit these vulnerabilities.

- **AI has expanded the playing field for attacks:** It is easier for adversaries to launch phishing, vishing, SMS, and social engineering attacks. They create more realistic email scams, develop deepfake videos, clone voices, and design convincing fake websites to deceive employees, steal data, and hold it for ransom. The World Economic Forum ranked cyberattacks among the top-five global risks in 2024 and projects cyber insecurity to remain a top-10 risk for the next decade.[1]

- **Data breaches are surging at an alarming rate:** They're driven by negligence, ransomware effectiveness, poor cybersecurity program management, open-source vulnerabilities, rapid innovation, and supply chain attacks. These breaches harm customer trust, trigger costly compliance violations, and jeopardize the very survival of businesses. Executives know that running and growing a business is significantly more challenging in the age of AI.

Our study shows that confidence varies across executive roles and levels, with technology and security executives expressing more reservations than CEOs about their security readiness. Most security leaders (76%) are increasing their budgets in 2025 to address growing risks and are prioritizing greater use of tools and products (85%), internal staff (64%), and external consultants (59%)[2]. CEOs, CIOs, and CISOs selected external consultants as their top choice for new spending, whereas tools and products were ranked highest by leaders with other titles and across all industry sectors.

Perception versus reality:
Security budgets increased by only 8% in 2024[3] despite the explosion of AI-powered threats, which require new strategies, skills, and talent to combat.

Companies grapple with executive and talent shortages and skills gaps, which disrupt their ability to set and evolve strategies, effectively assess risks, ensure a coordinated response to incidents, and strengthen their security posture. The US alone needs over 225,200 additional workers to fill 470,000 open cybersecurity jobs[4]—a figure that doesn't account for leader and staff burnout and frequent turnover. Digging deeper into the numbers, most of these job openings are for senior people with advanced skillset requirements, meaning that eager junior candidates won't be considered for these roles. While many C-suite leaders have the misconception that one person can do the work of many, one director-level information security person typically can't perform the functions of an entire team.

To combat these challenges, leaders are adopting an ecosystem approach. They are turning to virtual chief information security officer (vCISO) services and managed security service providers (MSSPs) to fill critical gaps, gain specialized expertise, and access critical capabilities on demand. This report examines the structure of security teams, their confidence in managing threats, challenges they face, breach findings, and areas where additional support is crucial. It provides executives with the actionable insights they need to evolve their programs and processes to address sophisticated threats in an era of weaponized data and AI.

Go It Alone or Seek Outside Support? How Organizations Are Staffing Their Security Teams

There's no single way to staff a security organization, reflecting companies' different industries, strategies, sizes, and budgets.

- **Teams have mixed compositions:** Most respondents either lean on a mix of in-house and contractor security work (39%) or entirely on their in-house teams (36%). Contractors help staff critical functions, such as security operations, without the obligation of hiring and development.
- **There's growing interest in external support:** A minority of respondents (13%) primarily rely on part-time or fractional roles, and 12% fully outsource external vendors. Although these numbers are modest, they highlight a growing trend toward seeking external support and expertise.

Industry	Combination (In-House and Contractor)	In-House	Part-Time/ Fractional	Fully Outsourced
Automotive	40%	60%		
Banking	36%	40%	9%	9%
Energy	50%	25%		25%
Finance	48%	19%	14%	19%
Fintech	50%	38%	13%	
Healthcare	32%	45%	18%	5%
High tech	34%	36%	14%	15%
Insurance	50%	25%		15%

Key findings:

- **Companies rely on multiple vendors for security:** Over three-quarters of respondents' organizations (77%) use 3-5 external vendors to manage their security programs, with finance, fintech, healthcare, and high tech leading the charge. This multi-vendor approach enables organizations to access best-of-breed expertise, specialized services, and 24/7 monitoring, while reducing the risks associated with relying on a single provider. This is contrary to the consolidation, or "platformization," of vendors and services that is occurring at an enterprise level.

- **Finance companies lead in embracing external cybersecurity support:** Finance firms outsource an impressive 81% of all security services, likely due to the complexities of monitoring extensive legacy systems. In contrast, fintech firms, often cloud-native with more modern infrastructures, outsource only 63% of their security needs. This difference highlights the unique security challenges faced by legacy-dependent industries compared to agile, cloud-first organizations.

Perception versus reality: **Vendor consolidation may simplify operations and reduce complexity, but it also increases strategic risk. Relying too heavily on a single partner can leave firms vulnerable if that partner falls short or has a critical vulnerability that affects their entire product line.**

- **Companies may be consolidating security vendors:** None of the respondents reported using six or more vendors, potentially indicating a trend toward vendor consolidation. However, 23% of companies are adopting a leaner approach, using just 1-2 vendors. Energy, finance, and high-tech industries are leading this trend, likely due to specialized processes or strategic partnerships with large, full-service providers. This shift may reflect executives' growing focus on efficiency, cost control, and streamlined security management.

Less Than 1 in 2 Leaders Feel Very Confident in Their Ability to Tackle Escalating Threats

Respondents expressed confidence about their ability to combat threats, but fewer revealed strong confidence in the face of rising AI-enabled attacks and a growing pool of adversaries.

- **Most leaders remain confident in their approaches:** Nearly all respondents (92%) stated they had some degree of confidence in their organization's ability to meet compliance requirements and tackle advanced threats with current staff and tools. This optimism likely stems from leaders' work to stay informed about industry trends and evolve strategies to address emerging risks effectively.

- **Strong confidence is less common:** Less than one in two leaders (48%) reported being very confident in their ability to combat threats, while 44% felt moderately confident. A smaller segment expressed neutral views (5%) or a lack of confidence (2%). This tempered optimism highlights the growing challenges executives face, including the rapid pace of technological change, the rising number of AI-empowered adversaries, and the increasing frequency and severity of data breaches.

Who's Most Confident In Their Organizations' Security Preparedness?

The closer the leader to the security program, the less likely they were to report that they were "very confident" it could withstand all threats.

CEOs	CIOs	CSOs
68%	31%	5%

- **Confidence levels differ across leadership roles:**
  - Two-thirds of CEO respondents (68%) reported being very confident in their organizations' ability to combat threats. This confidence likely stems from their role in hiring security leaders and shaping overarching strategies. However, their disconnection from the day-to-day realities of threat data and security responses may create a gap in their understanding of operational challenges.
  - CIOs bring a more grounded perspective. Only 31% said they were very confident, while 62% reported general confidence. Their hands-on insights into data protection challenges, particularly gaps stemming from legacy technology, provide a more realistic view of their organization's readiness.
  - CSOs expressed the most caution. Only 5% of CSOs said they were very confident, while the majority expressed moderate confidence or neutrality. As the leaders most directly responsible for security preparedness, CSOs are acutely aware of the gaps and challenges in current systems and processes.
- **A growing awareness of the need for external support:** With more than half of leaders uncertain about their organization's ability to address emerging risks, many are beginning to recognize the value of external expertise. Upgrading capabilities through partnerships, such as leveraging virtual CISOs or managed security services, could be a critical step toward strengthening defenses.

Perception versus reality:
While most CEOs express high confidence in their organization's security strategies, only 5% of CSOs share the same view. Who has the most realistic understanding of today's evolving threat landscape?

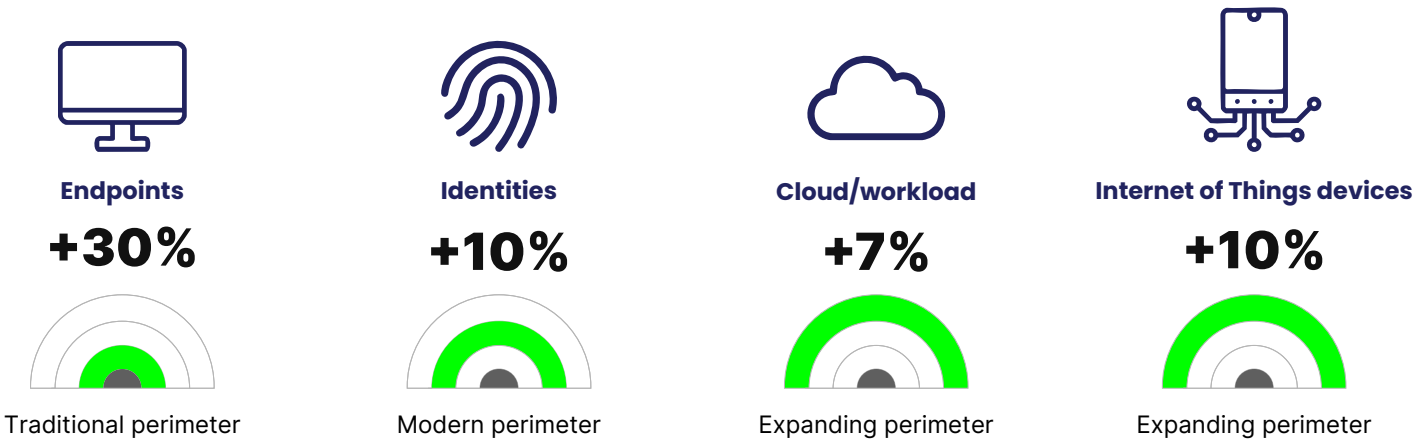
Cloud Security: #1 Challenge Outpacing Other Risks

The survey revealed that cloud security is the dominant challenge facing organizations, far surpassing other risks experienced this year. Leaders identified cloud and data security as top concerns due to the rapid shift to multi-cloud/hybrid-cloud infrastructures, which introduce complexity and create exploitable gaps for adversaries.

- **Cloud security is the #1 concern:** Business challenges and risks are growing, but leaders don't rank them equally. The #1 risk cited by 41% of all leaders (including 60% of CISOs and 56% of CEOs) was cloud security management. Leaders across energy, finance, fintech, healthcare, high tech, and insurance all selected this risk as their top concern. This surge is likely driven by companies accelerating their move to the cloud, building multi-cloud/hybrid-cloud infrastructures to modernize data, enhance analytics, and lay the groundwork for AI and machine learning innovation. However, this rapid transformation also increases complexity, creating vulnerabilities that adversaries can exploit. CIOs prioritize sensitive data and uptime. They were the only group to disagree, rating threats to sensitive data and company uptime as their greatest security challenge. Their focus reflects their role in enabling secure data sharing, supporting monetization initiatives, and ensuring the reliability of core systems.

Growing Businesses Have a Larger Attack Surface[5]

With more devices, people, cloud services, and connections, business risks and threats will skyrocket over the next three years.



Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

- **Real-world threat awareness shapes priorities.** CISOs, CEOs, and CTOs prioritized cloud security management significantly higher because of their proximity to threat data. Security directors, while also ranking cloud security highly, showed a more balanced concern for other risks, likely due to their focus on operational implementation.

73 days: Average amount of time it takes an organization to detect and contain threats,[6] giving malicious actors ample time to exfiltrate or manipulate data, or cause significant disruption.

- **Combatting threats to sensitive data and uptime:** Nearly one in four respondents (23%) ranked threats to sensitive data and company uptime as their second priority. CSOs were evenly split between this challenge and cloud security, reflecting their detailed understanding of data protection complexities. With the expansion of cloud infrastructures and AI applications, data copies are proliferating, increasing risks unless companies adopt advanced solutions like data federation to reduce the need for copying or confidential computing to securely process encrypted data.

- **Ensuring compliance with industry regulations:** Only 12% of respondents listed compliance as their top concern, placing it third. This lower ranking reflects the maturity of many organizations' compliance programs and the availability of cloud-native platforms offering continuous compliance capabilities, particularly for stringent frameworks like General Data Protection Regulation (GDPR).
- **Overcoming staff limitations and skill shortages:** Only one in 10 (10%) considered staff limitations and skill shortages a significant risk, ranking it fourth. This challenge may have been deprioritized due to the availability of talent from current economic conditions and technology industry layoffs, which have increased employee tenure and given CSOs a wider talent pool from which to hire.

Perception versus reality:
While leaders cited staff limitations and skill shortages as their #4 challenge, almost 2 in 3 security professionals reported feeling burned out.[7] This disconnect suggests leaders may be underestimating attrition risks and the actual head count required to address these challenges effectively.

- **An overlooked concern: Assessing third-party risk and cyber insurance requirements.** A surprising finding was that companies ranked third-party and cyber insurance requirements as their fifth security concern, with only 6% identifying it as a priority. This ranking stands in stark contrast to the growing reliance on external vendors, increased partner data sharing, and the rise in supply chain attacks.

  The low level of prioritization suggests that many organizations have yet to fully recognize the critical role cyber insurance and third-party risk management play in safeguarding against potential business disruptions caused by third-party breaches. Without adequate focus on this area, companies remain vulnerable to cascading effects from a partner's security failure, such as operational downtime, regulatory penalties, and reputational damage.

  This finding underscores a significant gap in risk perception that organizations must address as third-party ecosystems and supply chain complexities continue to expand.

Perception versus reality:
With third-party and cyber insurance deprioritized as the #5 risk, enterprises may be in for a costly surprise in the event of a data breach. The cost to remediate an enterprise data breach was $9.36M in 2024.[8] For firms with under 500 employees, the cost was $3.31M in 2023.[9]

7,000: The average number of suppliers that a technology company has, including 125 tier-one suppliers.[10]

- **Just 5% lack confidence: Are most overconfident?** Only a minority of respondents admitted to lacking confidence in their cyber strategies, a strikingly low figure. But does this minority reflect a more realistic perspective? The survey suggests that many leaders may be over-confident in their organizations' security preparedness, despite the growing sophistication of threats, leading to significant gaps or blind spots in their strategies, leaving organizations vulnerable to critical risks.

Nearly 1 in 2 Companies Breached in Past 12 Months

For many companies, the question isn't if a breach will occur but when and how severe it will be. The survey highlights that breaches remain a critical concern, even for organizations that claim strong confidence in their cybersecurity strategies.

- **1 in 2 companies have been breached:** Almost half of respondents (49%) said that their organization has suffered a security breach in the last 12 months, including data exfiltration, ransomware attacks, and unauthorized access. The findings underscore that no organization—no matter how advanced—is fully immune to the growing sophistication of cyber threats.

- **Finance and banking industries hit hardest:** Finance (57%) reported the most breaches, followed by banking (55%), reflecting the immense value of their customer data and high transaction volumes. These sectors remain prime targets for attackers, given their lucrative data sets and critical infrastructure. Most other industries were more evenly split between yes and no.

- **The automotive industry reports the fewest breaches:** The automotive industry experienced the lowest breach rate, with just 20% reporting an incident. However, 20% of respondents were unsure, suggesting a lack of visibility into potential bad actors within their multi-cloud/hybrid-cloud environments. While automotive companies currently don't yet have the rich treasure trove of sensitive data that other industries possess, the rise of fully autonomous vehicles and connected car systems will turn the sector into a more attractive target for cyberattacks.

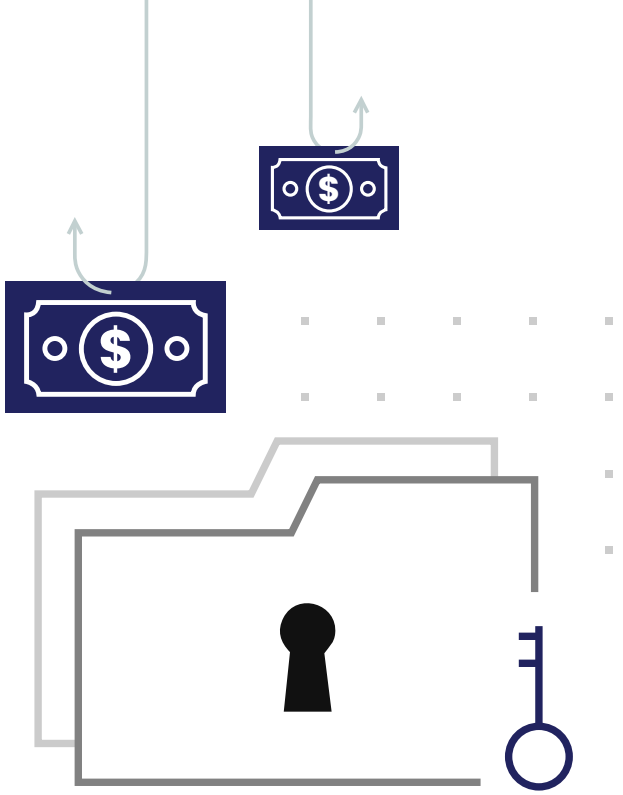
- **Executives' awareness of breaches varies by role.** Interestingly, awareness of breaches differed by leadership role:

CISOs: 100% of CISOs acknowledged breaches, reflecting their direct involvement in monitoring anomalies and incident data daily.

CEOs: Only 60% of CEOs were aware of breaches, highlighting a potential disconnect between security teams and top leadership.

CTOs and directors: These roles reported more "no" than "yes" responses, possibly due to limited communication from security teams or a lack of full visibility into breach incidents.

The rising cost of ransomware >$1.54 million:



The average cost of a ransomware payment surged in 2023, nearly doubling from $812K in 2022.[11]

Perception versus reality:
Businesses often over-rely on penetration tests to assess whether a breach has occurred. While useful, these tests don't reveal significant risks, such as privileged users who should have been offboarded but haven't.

Companies Need Support to Tackle Critical Security Imperatives

The rapid pace of technological and threat evolution demands that leaders continuously adapt their security strategies and programs. While challenges persist, the survey highlights several key areas where organizations are seeking support to strengthen their defenses:

- **Accelerating implementation to stay ahead of adversaries:** Nearly three in five respondents (58%) want to move faster to deploy new technologies and processes more quickly to match the speed of evolving threats. For example, many MSSPs offer cybersecurity as a service (CSaaS) capabilities, enabling customers to fill critical gaps and operationalize new technology investments swiftly.

- **Developing comprehensive strategies/programs amid talent shortages:** With cybersecurity talent shortages affecting all levels, from CSOs to junior recruits, 54% of respondents expressed a need for support in setting strategies and developing programs. This trend is especially pronounced in the energy sector. Organizations can turn to vCISO services to craft robust strategies, stabilize programs during leadership transitions, or prepare for rapid growth by laying the groundwork for their first executive security hires.

Perception versus reality:
By 2025, nearly half of all cybersecurity incidents will result from a lack of talent or human error, according to Gartner.[12] As a result, CSOs may be wise to set up the partnerships they need now to ensure the long-term success of strategic initiatives.

- **Capitalizing on specialized expertise to address advanced threats:** Companies have different needs based on their sector, business model, and size. So, it's unsurprising that more than one in two (52%) seek specialized expertise to address the latest threats. Customized MSSP services offer solutions to meet emerging requirements. These services include conducting risk assessments to identify critical vulnerabilities, evolving compliance programs to meet new data and AI requirements, and strengthening third-party risk management to safeguard against supply chain attacks.

- **Enhancing executive-level oversight and visibility:** Nearly half of leaders (45%) identified a need for improved executive-level oversight and visibility. Corporate security and technology leaders often struggle to secure buy-in from CEOs for new strategies, increased budgets, understanding insurance requirements, and responses to emerging threat patterns. vCISOs can bridge the gap, making a case for new investments and helping align security programs with broader business objectives and gain C-suite/board-level buy-in.

- **Addressing budget limitations while improving security:** CSOs don't have unlimited funds to address security imperatives. That's why nearly half (42%) say they'd like support addressing budget constraints while improving security. This was a top requirement for CSOs and a priority for directors. For many firms, it may be more cost-effective to partner with an MSSP or vCISO for needed services rather than staff up the organization, especially when a partner commits to an outcomes-based security model.

Perception versus reality:
Confusion between MSSPs and vCISOs persists, with 7% of leaders admitting they don't know the difference, and 8% incorrectly believing they are the same, with results consistent across industries. Surprisingly, some CSOs viewed them as similar. This misconception may prevent firms from leveraging vCISOs' strategic C-level expertise to elevate their security programs.

Why Companies Are Turning to MSSPs and vCISOs for Security Support and Expertise

As security challenges grow more complex, companies are increasingly partnering with managed security service providers (MSSPs) and virtual chief information security officers (vCISOs) to gain expertise, flexibility, and cost-effective solutions. Respondents highlighted several key benefits of working with MSSPs, revealing why these partnerships are critical for modern organizations:

- **Leveraging 24/7 monitoring and immediate incident response:** More than a third of respondents (37%) turn to MSSPs for 24/7 monitoring and rapid incident response, with automotive and insurance leaders prioritizing this for skilled talent, follow-the-sun coverage, and immediate action. CEOs value it most for their board reporting responsibilities.

  While MSSPs manage operations, vCISOs provide strategic oversight to ensure these efforts align with business goals. This combination strengthens security frameworks and addresses both immediate threats and long-term objectives.

- **Outsourcing full operational management of security functions:** Businesses may go all-in on innovation and outsource key functions like security. Nearly one in three respondents (32%) saw the value in outsourcing full operational management of security functions, a strength of MSSPs. However, organizations seeking business-aligned strategies and leadership during critical transitions often turn to vCISOs.

  vCISOs provide continuity during leadership gaps, help set long-term goals, and navigate periods of rapid growth or transformation. Their ability to function as an embedded security leader allows organizations to develop robust strategies that evolve alongside the business.

Perception versus reality:
Only 1 in 3 security leaders see MSSPs as a top choice for managing their security operations. However, more than 9 in 10 CEOs sought to accelerate transformational change in 2024[13] which may involve outsourcing non-core competencies.

- **Harnessing a cost-effective solution for day-to-day security tasks:** Budget-conscious leaders often turn to MSSPs for tasks like cloud security posture management, threat hunting, and tool rationalization. About 17% of respondents valued MSSPs as a cost-effective way to manage daily security operations.

  However, vCISOs play a critical role in ensuring these services align with the organization's overall strategy. They help optimize budgets by prioritizing investments, reducing redundancies, and ensuring outsourced services deliver measurable outcomes.

- **Obtaining specialized access to technical security resources and infrastructure:** About 14% of respondents rely on MSSPs for access to technical security resources and infrastructure, avoiding the time-consuming process of hiring and training staff and vetting new technology. MSSPs provide immediate access to advanced tools and skilled professionals, helping leaders bypass bidding wars and concerns about internal skill gaps. vCISOs also provide these resources and ensure they are strategically deployed to address specific vulnerabilities, compliance needs, and industry challenges.

Security Budgets Slated to Grow in 2025

3 in 4 businesses:

Among respondents, 76% of companies plan to increase security budgets in 2025, while 22% will maintain current spending levels, and only 2% anticipate reductions. For CSOs, this highlights the need to balance hiring and development priorities with addressing critical threats through vCISO and MSSP support.

vCISOs Offer Leadership on Demand

Hiring a full-time CISO can cost large companies up to $1M or more,[14] leading CEOs to prioritize other expenditures or defer the hire altogether. Virtual CISOs (vCISOs) provide an effective alternative, offering businesses access to seasoned security leadership and expertise without the long-term financial commitment. Respondents identified several key benefits of working with vCISOs:

- **Cost-effective access to seasoned security leadership:** vCISOs bring a wealth of expertise that businesses can harness to solve specific problems, such as vetting potential full-time hires, addressing critical risks, evolving third-party risk programs, and more. That's why one in four (28%) highlighted vCISOs as a cost-effective solution to seasoned security leadership without the cost of a full-time hire. CIOs were the leaders most concerned about enhancing security leadership with vCISO expertise while adhering to budget limitations.

Perception versus reality:
Only 1 in 4 leaders advocate hiring a vCISO for a season or a reason, such as an executive's departure. Yet, the average CISO tenure lasts just 18 to 26 months—and nearly half are expected to change roles in 2025.[15] These gaps in tenure create risks, such as the loss of security momentum and continuity, that a vCISO can address.

- **Flexible and scalable expertise on demand:** vCISOs operate on a retainer-based model, allowing businesses to pay for only the services they need while retaining the option to scale quickly, such as adding incident response capabilities. For this reason, nearly one in five (19%) say a major vCISO benefit is gaining the expertise they need when and how they need it. This answer was cited by most security leaders other than CISOs.

- **Improving strategic oversight and alignment with business goals:** vCISOs work closely with the C-suite to ensure cybersecurity strategies, support growth, and address the latest threats. Thus, around one in six (15%) say that vCISOs provide strategic oversight of security programs and ensure their continuous alignment with business goals, a top benefit cited by leaders across various roles.

- **Gaining guidance, compliance, and risk management expertise:** vCISOs bring an outsider's perspective, offering unbiased assessments of security programs and identifying gaps in risk management and compliance. This objective guidance was highlighted by 15% of respondents, with energy executives ranking it as the top benefit of working with a vCISO.

- **Temporary specialized expertise for organizational gaps:** vCISOs can provide high-level guidance to fill temporary organizational gaps, whether stepping in after a security leader's departure or supporting a mid-sized business preparing to hire its first senior security executive. As a result, more than one in nine (12%) cited this as a key advantage, with automotive, fintech, finance, and healthcare leaders particularly valuing this flexibility.

- **Addressing skills gaps without a full-time hire:** For some businesses, hiring a full-time CISO isn't practical or necessary. More than 11% of respondents noted that vCISOs, as fractional leaders, fill critical skills gaps without requiring a permanent role. This benefit was especially important to pharmaceutical leaders, who ranked it as their top choice.

While vCISOs can provide invaluable strategic expertise, they typically must be augmented with a team to execute their strategy. If businesses don't have sufficient staff on hand, they can supplement vCISO services with MSSP capabilities.

Collaborating to Address New Risks and Threats

As security leaders partner with other C-suite leaders to protect and grow their organizations, they can leverage external MSSP and vCISOs resources to help plug critical service gaps and gain valuable expertise to refine and evolve security strategies in the face of mounting threats.

However, leaders must address internal disconnects that could undermine progress, such as:

- Overconfidence in existing security strategies, despite the rising number of breaches.
- Overreliance on penetration tests instead of investing in comprehensive defenses.
- Limited understanding of the distinct roles MSSPs and vCISOs play in strengthening security.

Leveraging the Value of MSSPs and vCISOs

The good news is that across roles and industries, executives understand the value of MSSPs in extending service coverage or even serving as an outsourced security partner. Likewise, they see vCISOs as valuable assets. vCISOs provide seasoned security leadership that aligns with business strategies, improves risk and compliance capabilities, and delivers other gains.

As risks and threats increase, companies are harnessing the power of the ecosystem. They're leveraging partners such as Cyber Defense Group for MSSP and vCISO services to assess their preparedness, adopt new tools and processes to improve their security posture, and accelerate incident response.

CDG | CYBER DEFENSE GROUP

Empowering Businesses with Expert-led Security Services

A partnership with Cyber Defense Group delivers enterprise-grade cybersecurity capabilities at a fraction of the cost of full-time staffing.

- **Outcomes-based programs:** Achieve measurable results with tailored security strategies aligned to business objectives.
- **Expert team versus a single vCISO:** Access a full team of seasoned experts, providing comprehensive support or augmenting your existing staff.
- **Agile, top-tier expertise:** Gain industry-leading insights with the adaptability of a boutique provider that comes with a skilled, seasoned full-stack security team.
- **Fixed, predictable costs:** Secure top-tier services with transparent, competitive pricing to maximize your investment.

Together, these solutions empower businesses to innovate securely while staying ahead of advanced threats.

Take the next step toward cyber resilience

Learn how external partners can transform your security strategy. Contact us for a complimentary 60-minute discovery call to explore how we can help your organization thrive and grow amidst a challenging cybersecurity landscape.

Sources

1 The Global Risks Report 2024, 19th Edition, World Economic Forum, pages 7-8, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

2 CensusWide conducted an independent survey of 300 U.S. IT security professionals in November 2024 for the Cyber Defense Group.

3 "New Research Reveals Security Budgets Only Increased 2 Points in 2024, While 12% of CISOs Faced Reductions," press release, IANS, September 5, 2024, https://www.iansresearch.com/resources/press-releases/detail/new-research-reveals-security-budgets-only-increased-2-points-in-2024--while-12--of-cisos-faced-reductions

4 Nathan Eddy, "Cybersecurity Talent Shortage Prompts White House Action," article, Dark Reading, September 6, 2024, https://www.darkreading.com/cybersecurity-operations/cybersecurity-talent-shortage-prompts-white-house-action

5 Justin Greis and Marc Sorel with Julian Fuchs-Souchon and Soumya Banerjee, "The cybersecurity provider's next opportunity: Making AI safer," article, McKinsey, November 14, 2024, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer

6 "The cybersecurity provider's next opportunity," McKinsey, ibid.

7 "Report: 63% of security practitioners experience burnout," article, Security Magazine, August 26, 2024, https://www.securitymagazine.com/articles/100976-report-63-of-security-practitioners-experience-burnout

8 Cost of a Data Breach Report 2024, IBM, page 9, https://www.ibm.com/reports/data-breach

9 Cost of a Data Breach Report 2023, IBM, as cited in Andrew Rinaldi, "The Cost of Cybersecurity and How to Budget for It," article, Business.com, August 13, 2024, https://www.business.com/articles/smb-budget-for-cybersecurity/

10 Thomas Baumgartner, Yogesh Malik, and Asutosh Padhi, "Reimagining industrial supply chains," article, McKinsey, August 11, 2020, https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/reimagining-industrial-supply-chains

11 Daniel Thomas, "Report: Ransomware payouts and recovery costs went way up in 2023," article, SC Media, August 7, 2023, https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023

12 "Growing threats outpace cybersecurity workforce," article, Thomson Reuters, January 30, 2024, https://legal.thomsonreuters.com/blog/growing-threats-outpace-cybersecurity-workforce/

13 Andrea Guerzoni, Nadine Mirchandani, and Barry Perkins, "Should CEOs double-down on business transformation in the face of uncertainty?," report, E&Y, January 30, 2024, https://www.ey.com/en_gl/ceo/ceos-double-down-on-business-transformation

14 Sydney Lake, "Chief information security officers land nearly $1 million pay packages," article, Fortune, August 26, 2022, https://fortune.com/education/articles/chief-information-security-officers-land-nearly-1-million-pay-packages/

15 Mary K. Pratt, "The Rise In CISO Job Dissatisfaction – What's Wrong And How Can It Be Fixed?," article, Cybersecurity Ventures, April 24, 2024, https://cybersecurityventures.com/the-rise-in-ciso-job-dissatisfaction-whats-wrong-and-how-can-it-be-fixed/

CDG | CYBER DEFENSE GROUP

About Cyber Defense Group

At Cyber Defense Group, our vision is to revolutionize how small and medium-sized enterprise (SME) businesses perceive and engage with cybersecurity. We aim to cultivate a culture where customer obsession is paramount, and exceptional service is the norm. Our goal is to empower businesses, particularly in the SME sector, to gain a competitive edge by fully embracing cyber resilience. We envision a future where our clients are not only protected but are thriving and leading in their industries, thanks to robust, forward-thinking cybersecurity strategies.

For more information:

info@cdg.io www.cdg.io +1 (888) 450-0911