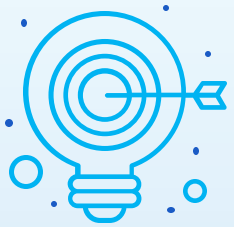# State of the Virtual CISO 2024

Why most MSPs and MSSPs will soon offer vCISO services

September 2024

# Table of **Contents**

# Introduction and Key Findings

# Introduction & Methodology

**When it comes to cybersecurity, small and medium-sized businesses (SMBs) recognize that no-one is safe.** Every organization, no matter its size, is now a target. Tasked with protecting their own customers in a supply chain that is only getting more complex, keeping up with compliance mandates that can often feel like moving targets, and jumping through hoops to meet the frameworks required by cyber insurance companies, it's never been more important for SMBs to close up their cybersecurity gaps.

**On this backdrop, it's no surprise that the Virtual CISO (vCISO) market is gaining significant traction**, allowing SMBs to gain the benefits of security knowledge, expertise and technology, without the heavy investment of onboarding a full-time CISO in-house. For Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs), offering vCISO services will soon be table stakes.

**At Cynomi, we believe that information about the opportunities of a vCISO solution belong to everyone**, and as thought leaders in this space, we are focused on collecting and sharing the data that supports service providers and their business growth. For the second year in a row, our State of the Virtual CISO Report asks MSPs and MSSPs where they are on their vCISO roadmap. We invite them to share the challenges they are facing in their business, the level of demand they see for cybersecurity services, the blockers they are experiencing to vCISO adoption, and for those who are already offering vCISO services – the results they are experiencing, as well as how these align with their strategic goals.

## Methodology

To understand the true state of the vCISO market we commissioned a survey of 200 senior security leaders from the U.S. and Canada, split evenly between MSSP and MSP companies. These respondents include CEOs, CIOs, CISOs, COOs, vCISOs, Heads of Security and Senior Security Consultants. We screened for IT companies with 50 or more employees that provide cybersecurity strategic services or cybersecurity consulting.

The survey was completed by Global Surveyz, an independent survey company, and took place during June and July 2024. The respondents were recruited through a global B2B research panel, and invited via email to complete the survey. The average amount of time spent on the survey was 6 minutes and 14 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

# Key Findings

**01 More than one fifth of MSPs and MSSPs are now offering vCISO services**

The importance of Virtual CISO (vCISO) services is gaining a lot of traction with today's service providers, and is almost ubiquitously on the organizational roadmap. Last year, 19% of MSPs and MSSPs were offering vCISO services, while this year that percentage has grown to 21%. In addition, of the remaining 79% who do not currently offer them, 98% plan to offer vCISO services to their clients in the future, and 39% are in the final stages of the process, planning to have vCISO services to offer by the end of 2024, if not earlier.

**02 The top benefits of vCISO services overlap with organizations' most strategic goals**

When we asked service providers who offer vCISO services about the benefits they experience, we found a tight overlap between those benefits and the wider strategic goals that service providers are looking to achieve over the next 12 months. Those who have a vCISO offering see growth in areas including the amount of recurring revenue they generate, the ease of upselling opportunities, the depth of customer engagement, their overall margins, and their ability to achieve true differentiation in their market.

**03 Those who don't offer vCISO services cite valid, but addressable objections**

Those who do not currently offer vCISO services cite issues such as technology or knowledge gaps in cybersecurity or compliance, as well as lack of skilled personnel, or a high initial investment. In reality, a vCISO platform would solve all of these issues and more, offering built-in CISO-level expertise, a low barrier to entry, and making it easier to sell vCISO services as well as other solutions by shining a light on any gaps in cybersecurity and compliance.

# Key Findings

**04** **Those who do offer vCISO services see the benefits on core business metrics**

Offering vCISO services positively impacts the customer and the service provider, too. 46% of service providers that offer vCISO services say there has been an improvement in their customer's security, and 44% say they see a boost in customer engagement. Behind the scenes, the impact is also measurable on margins and revenue. 37% of service providers who offer vCISO services clearly state they have increased their margins, and 34% saw increased revenues as a result of this service.

**05** **Both MSPs and MSSPs are overwhelmed by compliance frameworks and cybersecurity regulation**

93% of service providers say that they are overwhelmed by the complexity of cybersecurity frameworks such as NIST, NIS, and ISO. 74% feel the same way about broader data privacy and compliance mandates including GDPR, HIPAA and PCI-DSS. A vCISO platform would be a smart route to reducing the complexity, as one of its key functions is to map all frameworks and controls into an actionable plan for compliance. 33% of those who already use a vCISO platform call easy access to compliance frameworks a top benefit.

**06** **94% of service providers see the demand for vCISO services**

75% of MSPs and MSSPs see a high demand in the market for vCISO services, and a further 19% see a moderate demand. With 46% of service providers that have 500 or more employees making it a strategic priority to expand their cybersecurity offerings as an MSP or MSSP in the next 12 months – it's an exciting time to be adopting a vCISO platform, streamlining the journey to cybersecurity resilience for their clients alongside championing internal business growth.
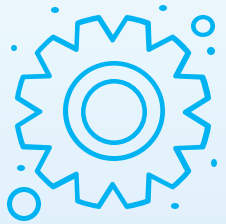
# vCISO Services

# 21% of MSPs and MSSPs are Already Offering vCISO Services

**Offering vCISO services is a growing trend, up from 19% in 2023 to 21% this year.**

The top cybersecurity service currently provided by MSPs and MSSPs is pentesting, offered by more than double the number of service providers as any other service.

For service providers who would like to expand their cybersecurity offering, **pentesting can be used as a springboard for discussion of wider vCISO services**. By upselling from the results of the pen test, MSPs and MSSPs can show the client that continuous risk assessment via vCISO services will provide greater visibility and resilience than a point-in-time pen test.

vCISO platforms can add true value to the client, and **automate manual processes and tasks to provide a wider range of solutions to** drive cyber resilience, including covering services such as cyber insurance readiness, compliance readiness and monitoring, and risk assessment.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%*

| Service | % |
|---|---|
| Pen testing | 47% |
| Cyber insurance readiness | 23% |
| External attack surface management | 23% |
| Extended Detection & Response (XDR) | 22% |
| Dark web monitoring | 22% |
| Managed Detection & Response (MDR) | 22% |
| Compliance monitoring and readiness | 21% |
| Patch management | 21% |
| vCISO services | 21% |
| Security awareness & training | 20% |
| Risk assessment | 19% |
| Incident Response (IR) & forensics | 19% |
| Managed SIEM / SOC | 16% |
| Threat intelligence | 15% |

*Figure 1: Top Product and Services Offered by MSP/MSSPs*

# 98% of Service Providers without vCISO Services Plan to Offer These in the Future

**Of the service providers who do not currently offer vCISO services, just 2% say they have no plans to provide this offering to their clients in the future.**

This shows a strong recognition in the industry of how important vCISO services are to small and medium-sized businesses (SMBs).

**39% of service providers are planning to add vCISO services to their offering within the next few months,** and a further 35% will do so before the end of 2025.

With such a strong drive towards onboarding vCISO services, MSPs and MSSPs without this offering on their roadmap may soon find themselves at a disadvantage.
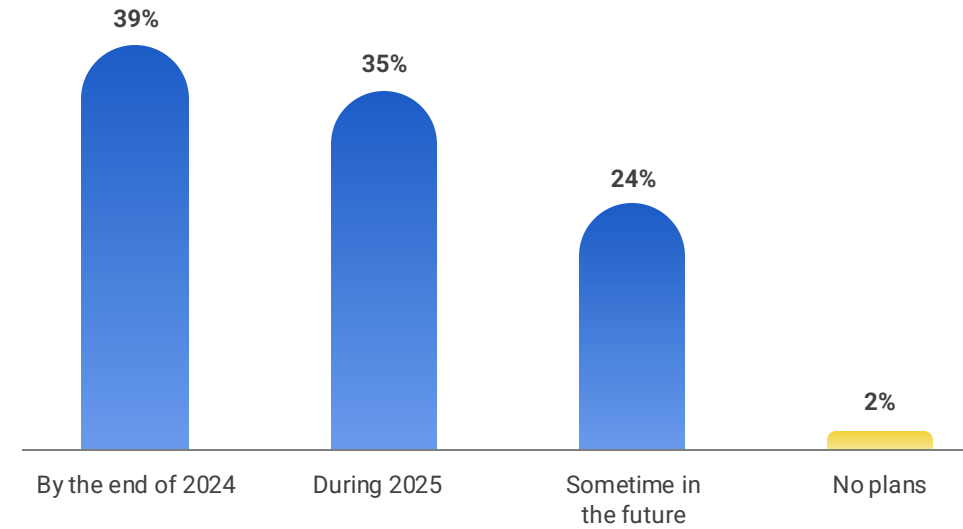


*Figure 2: Timeline for Offering vCISO Services*

# 43% of MSPs and MSSPs Believe that vCISO Services will Improve Customer Security

There are a wide range of different benefits that service providers see when they implement vCISO services, with the top three being **an improvement to customer security (43%), the ability to upsell other products and services (38%), and a directly positive impact on recurring revenue (37%).** In addition to improving clients' cybersecurity, there is a clear perception among service providers that vCISO services positively impact the business behind the scenes, allowing for easier upsell, recurring revenue growth, client engagement and differentiation.

If we compare these benefits to the strategic goals of today's service providers, (Figure 11) we can see a strong overlap. As a result of the multi-faceted value to service provides, **MSPs and MSSPs are increasingly turning to vCISO services as a way to meet their core goals, from customer engagement and upsell opportunities, to direct revenue growth and differentiation.**

*Question allowed more than one answer and as a result, percentages will add up to more than 100%*

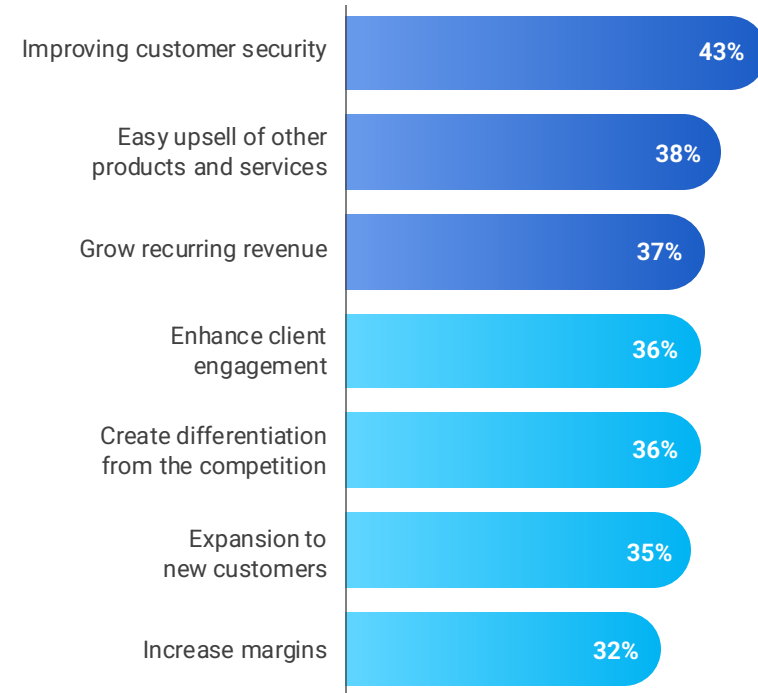| Benefit | Percentage |
|---|---|
| Improving customer security | 43% |
| Easy upsell of other products and services | 38% |
| Grow recurring revenue | 37% |
| Enhance client engagement | 36% |
| Create differentiation from the competition | 36% |
| Expansion to new customers | 35% |
| Increase margins | 32% |

*Figure 3: Top 3 Benefits of Adding vCISO Services to an MSP/MSSP Offering*

# What's Holding Service Providers Back from Offering vCISO Services?

**Service providers have many reasons that they claim are stopping them from offering vCISO services, but how valid are those reasons?**

It's interesting to see how many MSPs and MSSPs believe they need a lot of knowledge around security or compliance to offer a vCISO service. In reality, this perception is untrue, as with a vCISO platform – the knowledge is inherent in the solution.

In fact, a vCISO platform can solve a number of these blockers, such as a lack of skilled personnel, the limited headcount, or the weight of too many time-consuming tasks. **A vCISO platform allows service providers to offer vCISO services at lower cost and with greater ease**, and even makes it easier to sell vCISO services as well as other solutions by highlighting gaps in cybersecurity and compliance.

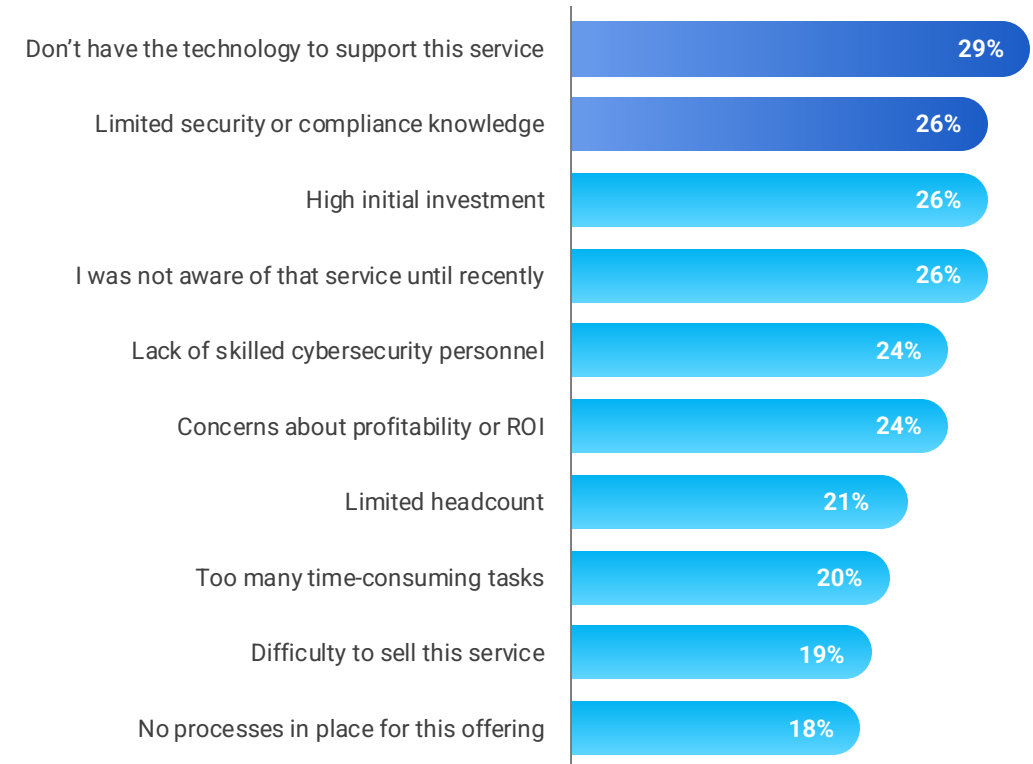*Question allowed more than one answer and as a result, percentages will add up to more than 100%*

| Reason | Percentage |
|---|---|
| Don't have the technology to support this service | 29% |
| Limited security or compliance knowledge | 26% |
| High initial investment | 26% |
| I was not aware of that service until recently | 26% |
| Lack of skilled cybersecurity personnel | 24% |
| Concerns about profitability or ROI | 24% |
| Limited headcount | 21% |
| Too many time-consuming tasks | 20% |
| Difficulty to sell this service | 19% |
| No processes in place for this offering | 18% |

*Figure 4: The Primary Reasons for Not Offering Virtual CISO Services*

# 93% of Service Providers are Overwhelmed by Cybersecurity Frameworks

One of the roles of the vCISO is to help the organization to manage the complexity of compliance and cybersecurity frameworks.

Despite that, **74% of respondents feel overwhelmed by regulatory compliance frameworks such as PCI-DSS or GDPR, and 93% feel overwhelmed by cybersecurity frameworks including NIST or ISO.** Just 2% say that they are not overwhelmed at all by regulatory compliance frameworks and none said they are not overwhelmed at all by cybersecurity frameworks.

When we drill down into the number of service providers who feel only slightly overwhelmed by cybersecurity frameworks, we see that more MSPs feel slightly overwhelmed compared with MSSPs. Managed Service Providers are mainly handling IT solutions, while Managed Security Service Providers are focused on security, and yet **the data shows that MSSPs are more overwhelmed by cybersecurity frameworks than MSPs.** This may suggest that they feel the scope of what they have to deal with more acutely than their MSP counterparts.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%*
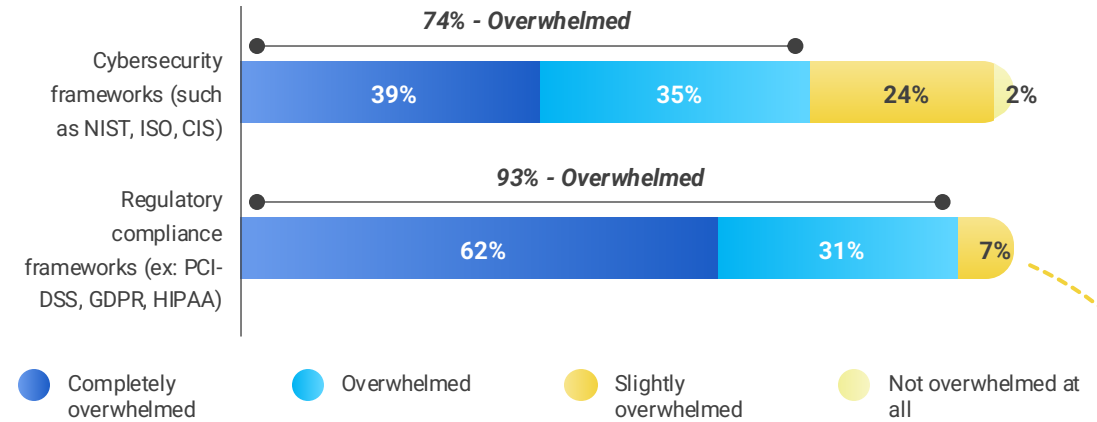


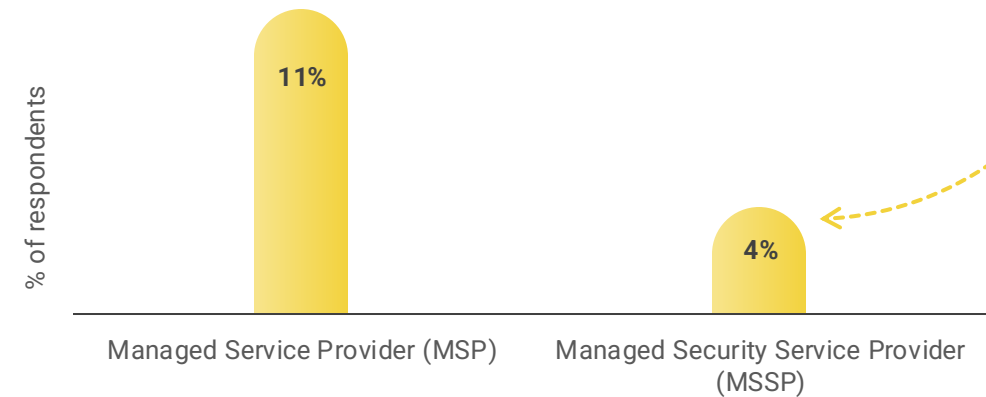Figure 5: Perceptions of Complexity in Cybersecurity and Regulatory Compliance Frameworks



Figure 6: 'Slightly overwhelmed' for " Cybersecurity frameworks", by Company Type

# The Majority of Service Providers that Offer vCISO Services See Increase in Revenue or Margins

**The majority of service providers who offer vCISO services see an increase in margins and revenues.** Overall, for 37%, offering vCISO services increases margins, and for 34%, offering vCISO services increases revenue.

When we look deeper at the data, 78% of service providers that mentioned they experienced a revenue increase have seen an increase of 20% or more in revenue by offering vCISO services. 67% of service providers that mentioned they saw an increase in margins, have experienced an increase of 20% or more when comparing their margins before and after adoption.

However, the impact of vCISO services is not only for the MSP or MSSP to grow their own business. It also has a strong impact on the end customer. **46% of respondents said their customer security was improved, and 44% noted that client engagement has taken a leap.**

vCISO services are a powerful business opportunity for MSPs and MSSPs, if they can overcome initial perceived barriers to adoption.

*\*Question allowed more than one answer and as a result, percentages will add up to more than 100%*



| | |
|---|---|
| Improving customer security | 46% |
| Increased client engagement | 44% |
| Increased margins | 37% |
| Upsell of other products and services | 37% |
| Increased revenue | 34% |
| Increase in customer base | 32% |
| Easier outreach to new customers | 32% |

*Figure 7: Impact of Offering vCISO Services*



% of respondents

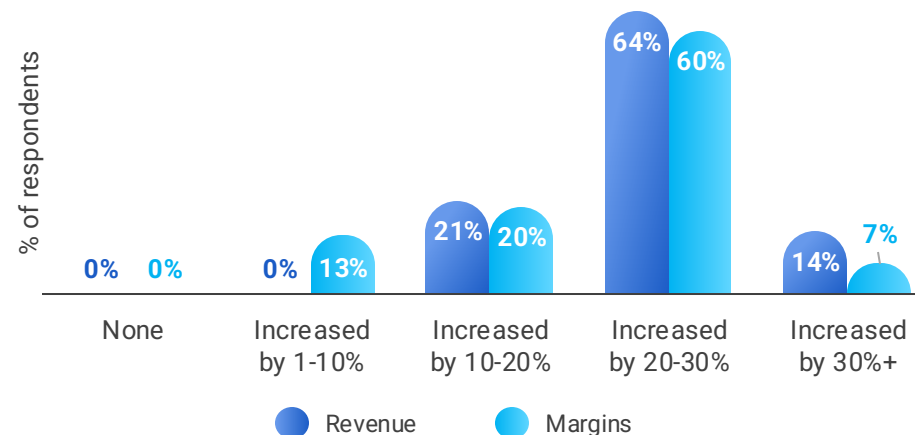| | None | Increased by 1-10% | Increased by 10-20% | Increased by 20-30% | Increased by 30%+ |
|---|---|---|---|---|---|
| Revenue | 0% | 0% | 21% | 64% | 14% |
| Margins | 0% | 13% | 20% | 60% | 7% |

● Revenue  ● Margins

*Figure 8: Increased Revenue & Margins from Offering vCISO Services, 2023*

# A Third of Service Providers See the Operational and Financial Benefits of Using a vCISO Platform

For service providers who use a dedicated vCISO platform, the benefits are clear. **34% see standardization of work processes, and 34% also enjoy accelerated onboarding of their new employees**, underscoring the importance of team efficiency as a core value. For service providers who do not have a dedicated vCISO platform, these are likely to be top administrative challenges.

In addition, **33% cite easy access to compliance frameworks, drawing a direct line to solve the challenge of figure 6 – the inherent complexity of managing compliance frameworks.**

Highlighting the business benefits, 33% of service providers using a vCISO platform have experienced an increase in revenue by being able to sell more vCISO services, and **32% call out the ability to upsell more widely across all of their products and services.**

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

| Benefit | % |
| --- | --- |
| Standardization of work processes | 34% |
| Accelerated onboarding of new employees | 34% |
| Easy access to multiple compliance frameworks | 33% |
| Increased revenue by selling more vCISO services | 33% |
| Easy upsell of other products and services | 32% |
| Shorter time-to-value for customers | 28% |
| Improved operational efficiency | 25% |
| Showing clear value to customers | 25% |
| Access to specialized expertise | 22% |

*Figure 9: Main Benefits of Using a vCISO Platform*

# 2025 vCISO Landscape

# The Larger the Service Provider, the More Likely They are to Expand on Cybersecurity in 2025

We asked service providers to name their top strategic focus areas for the next 12 months. 33% mentioned improving operational efficiencies, 31% would like to expand their cybersecurity services, and 29% are looking to increase sales and sell a broader variety of products and services.

**When service providers look to the future and define their key focus areas – it's interesting to note how many align with the same benefits that they can receive from offering vCISO services.**

Looking specifically at the drive to expand cybersecurity offerings, we broke the data down by company size, and found that **larger service providers are more likely to be considering expanding their cybersecurity service offerings in 2025 than their smaller peers.** 24% of companies with fewer than 200 employees are looking at expansion, compared with 46% of companies with more than 500 employees in-house.

It seems like the larger players see the expansion into cybersecurity as a strategic focus that will allow them to differentiate and grow their business.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%*



Improve operational efficiency — 33%
Expand cybersecurity services offerings — 31%
Increase sales to existing clients — 29%
Sell a broader variety of products and services — 29%
Differentiate from the competition — 28%
Ensure customer security — 26%
Grow recurring revenue — 22%
Enhance customer engagement — 22%
Improve profitability — 21%
Add new clients — 20%

*Figure 10: Strategic Focus for the Next 12 Months*



<200 employees — 24%
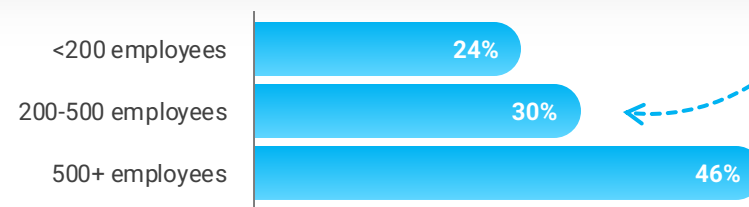200-500 employees — 30%
500+ employees — 46%

*Figure 11: Expansion of Cybersecurity Services Offerings by Company Size, 2024*

# 75% See High Demand for vCISO Services Among Their Customer Base

**Service providers recognize the demand among their clients for vCISO services, with 75% saying they are in high demand, and a further 19% citing they are in moderate demand.**

If we look further at the other cybersecurity services that are in demand, including strategic cybersecurity management and planning, compliance readiness, insurance readiness and cyber risk assessment – all of these can be offered by leveraging a vCISO platform, empowering MSPs/MSSPs to meet client demand and grow their business.

Looking at the high demand for cyber risk assessment, MSPs and MSSPs can use this approach to upsell vCISO services, too. Similar to what we saw with pentesting in figure 1, a risk assessment is often a one-time offering, which can then be leveraged to suggest wider cybersecurity services under a vCISO offering to enable clients to see true business resilience.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%*
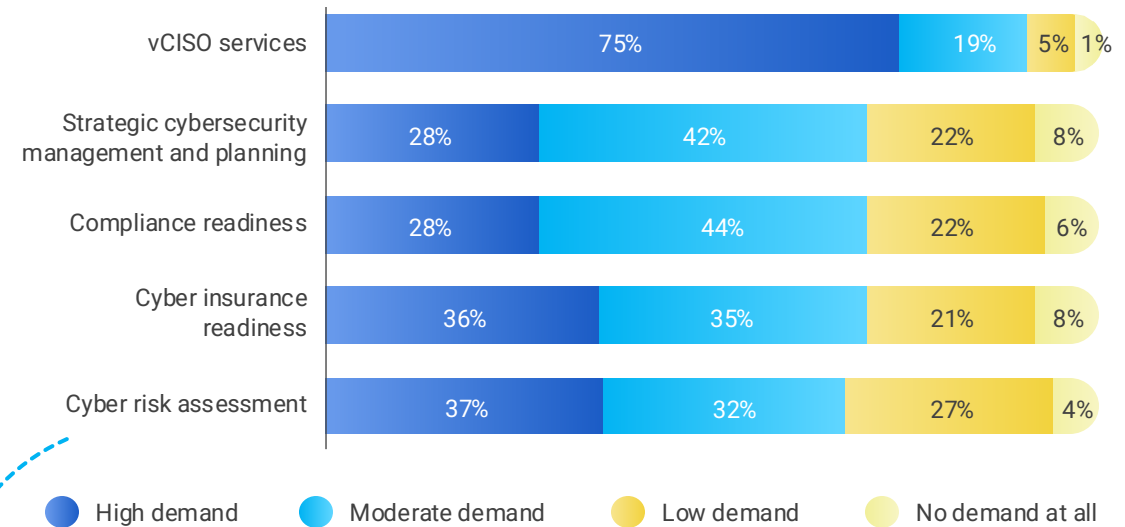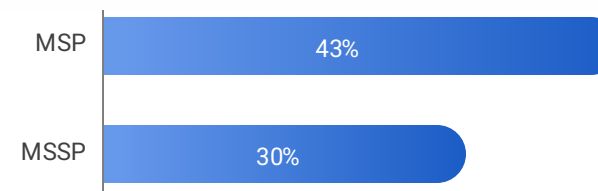


Figure 12: Top Demanded Cybersecurity Services



Figure 13: 'High Demand' for "Cyber Risk Assessment", by Company Type

# Demographics

# Country,
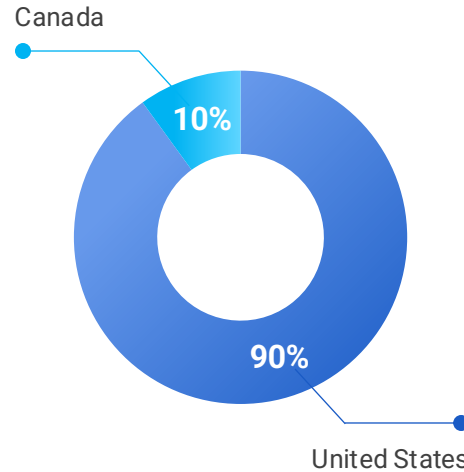# Company type,
# Company size,
# Job seniority,
# Job title



Figure 14: Country


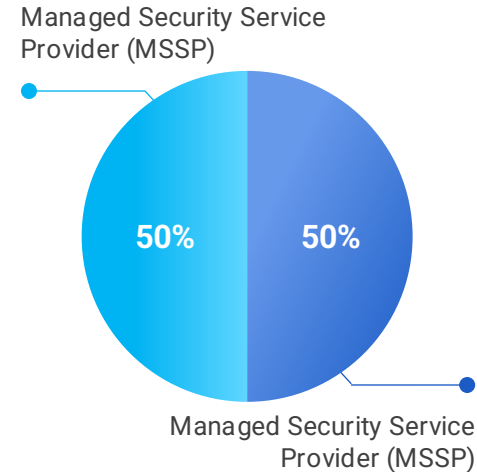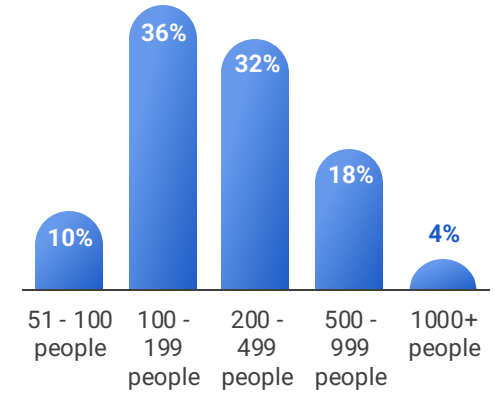
Figure 15: Company type



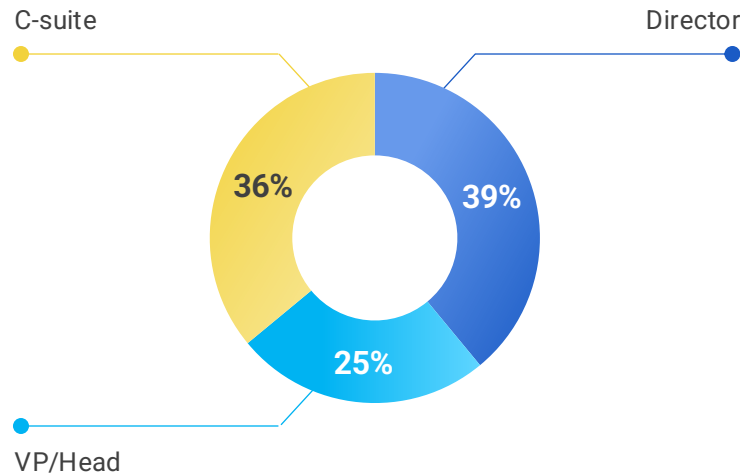Figure 16: Company size
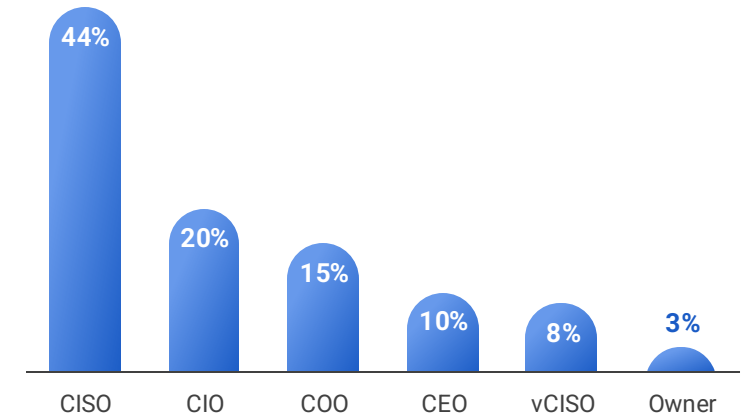


Figure 17: Job seniority



Figure 18: C-suite job function

# About Cynomi

Cynomi's AI-driven vCISO platform empowers MSSPs, MSPs and consultancies to offer structured cybersecurity services to SMEs at scale and provide them with proactive cyber resilience.

Combining proprietary AI algorithms with CISO-level knowledge and knowhow, Cynomi's vCISO platform streamlines service providers' cybersecurity management work while automating manual time-consuming tasks including risk assessment, compliance readiness, cyber posture reporting, creation of tailored security policies and remediation plans, as well as task management optimization.

Cynomi helps partners overcome the cybersecurity skill gap and scale their business, allowing them to offer new services, upsell and increase revenues while reducing operational costs.

The company was founded by David Primor, a former Lt. Colonel in IDF unit 8200 and the Technology Executive Director of Israel's cyber authority, and Roy Azoulay, a serial entrepreneur who founded and headed Oxford University's startup incubator, with the vision 'CISO-level cybersecurity for all'. Cynomi has offices in Israel, the UK, and the USA. To learn more about Cynomi's solution for MSPs, MSSPs, and cyber consultancies, visit www.cynomi.com.

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/virtual-ciso

to learn more.