



State of the Virtual CISO 2023 Report

How MSPs and MSSPs capitalize on the rising vCISO trend

August 2023

Table of Contents

Key Findings and Introduction	03
Report Findings	08
Most MSPs and MSSPs Are Already Offering Components of a vCISO Solution	09
86% of Companies Currently Offer or Are Planning to Offer vCISO Services by the End of 2024	10
Top Benefits of vCISO Services Validate Their Impact on Business Growth	11
Top Benefits of vCISO Services Are Aligned with Main Strategic Focus Over the Next 12 Months	12
Top Challenges in Providing vCISO Services	13
91% of Companies Believe Offering vCISO Services Requires Hiring Cybersecurity Experts, while 63% Cannot Afford to Hire Them	14
Most vCISO Tasks Are Time-Consuming	15
Demographics	16
About Cynomi	19





Key Findings and Introduction

Key Findings

01

The number of security-focused MSPs providing virtual CISO services will grow fivefold by next year

The vCISO trend is fairly new. It kicked off in earnest when 5% of MSPs and MSSPs began offering vCISO services in 2021 or earlier, and has been growing steadily since, with 8% offering them in 2022, 28% in 2023, and a projected 45% are planning to offer them in 2024 (Figure 3). By the end of 2024, it is anticipated that only 14% will not be offering vCISO services.

Overall, with 86% of security-focused MSPs and MSSPs either currently offering vCISO services (19%) or planning to offer them by the end of 2024 (67%), it's clear that the vCISO trend is decidedly 'hot', and those who fail to act on it well before the end of 2024 risk falling behind competitors who will already have a vCISO offering in place.

02

Top vCISO benefits center on business growth, which also aligns with the most pressing strategic goals for MSPs and MSSPs, reinforcing the urgency of introducing a vCISO offering to remain competitive

Adding a vCISO solution can help MSPs and MSSPs achieve their strategic goals (Figure 5), namely expanding their cybersecurity services offerings (39%), improving operational efficiency (36%), and improving profitability (32%). It also enhances customer engagement (31%), since vCISO services encompass strategy, which by default involves clients' C-level management, rather than the IT or operations stakeholders alone.

According to respondents, the biggest benefits of adding vCISO services to their offering (Figure 4) include an easier upsell of other products and services (44%), increased margins (43%), and improving customer security (42%). This is no surprise, given that many MSPs and MSSPs – who are typically margin-driven – are moving towards security, because they see it as their path to growth. Offering vCISO services can help them achieve both their margin targets and their cybersecurity targets, which explains the rising vCISO trend and reinforces the urgency for service providers to add a vCISO solution to their services stack to remain competitive.

03

Despite recognizing the benefits of adding a vCISO offering, service providers cite limited in-house security and compliance expertise, high upfront investment, and cybersecurity skill gap as the top barriers to entry

MSPs and MSSPs cited limited security or compliance knowledge (40%), high initial investment (34%), lack of skilled cybersecurity personnel (33%), limited customer maturity (31%) and too many time-consuming tasks (30%) as their top challenges in adding a vCISO offering as part of their service (Figure 6).

Many of these challenges can potentially be alleviated with vCISO platforms that leverage cybersecurity and/or compliance knowledge to automate most of the manual work and streamline the process.

Key Findings

04 **91% of companies believe that offering vCISO services requires hiring cybersecurity experts, while 63% cannot afford to hire them**

vCISO-related tasks are typically very time-consuming (Figure 9), so given that “limited in-house security or compliance knowledge” and the “lack of skilled cybersecurity personnel” were rated by MSPs and MSSPs as their top barriers to adding a vCISO offering (Figure 6), it makes sense that 91% of service providers agree that growing their vCISO services or adding this service to their offering will require hiring additional cybersecurity personnel to “some” or “a great” extent (Figure 7).

Unfortunately, almost two-thirds of respondents think their companies cannot afford hiring new cybersecurity experts (Figure 8), demonstrating that recruiting these experts is a key barrier to entry. While it is true that traditionally, vCISO tasks require special expertise and are labor intensive (Figure 9), emerging vCISO platforms help close this gap by automating most of the tasks, reducing the required time investment by 50-80% and saving hundreds of work hours per month. It’s therefore a myth that providing vCISO services necessitates adding expensive cybersecurity headcount.

05 **Most MSPs and MSSPs already offer components of vCISO, so they could potentially repackaging them into a lucrative vCISO offering**

Although the concept of vCISO services is fairly new, 19% (almost one in five) of MSPs and MSSPs are actively offering it as a solution. Larger service providers are leading the trend of offering vCISO services (Figure 2), but smaller ones are expected to follow, especially now that using vCISO platforms eliminate many of the barriers to entry.

Many service providers, however, are already offering components of the vCISO service (Figure 1), most notably security awareness and training (31%), compliance monitoring and readiness (30%), and risk assessment (26%). This means that they too could easily repackage these components and offer them as a comprehensive vCISO service, creating a new recurring revenue stream, differentiating themselves from competitors and growing their business.

Introduction & Methodology

Although the concept of Virtual CISOs (also known as Fractional CISOs or CISO as a Service) is fairly new, it has been gaining significant traction since 2021. Prior to that, CISOs – who generally command very high salaries¹ – were usually only engaged by large companies, as SMB budgets typically paled by comparison. But with small businesses now accounting for 43% of cyber-attacks annually,² they are more vulnerable and in need of protection than ever.

Most SMBs, however, usually lack the expertise to deal with threat detection and mitigation themselves. To manage their security posture effectively, they need to engage someone who has a holistic view of their tech infrastructure and is accountable for their cybersecurity and compliance. And since tools alone – however abundant – cannot properly ensure their protection, they tend to reach out to MSPs and MSSPs for assistance. In fact, according to a 2022 report by ConnectWise³, 94% of SMBs would consider using or moving to a new MSP if they offered the “right” cybersecurity solution.

MSPs and MSSPs understand there is a growing need from SMBs and SMEs that are looking for strategic guidance in addition to tools and are unable to afford a full-time CISO – but they aren’t necessarily aware of how to leverage this need, especially when they lack the necessary expertise. Leveraging automation to offer more efficient vCISO services is therefore the ideal solution, because it empowers them to provide proactive cyber resilience at scale without increasing

headcount. And it’s a win for SMBs too, because while a full-time CISO can command an average total pay package of \$215,000, SMBs can get a vCISO service to address their cybersecurity needs for a fraction of this cost⁴.

With the number of MSPs providing vCISO services set to grow fivefold by 2024, the rising vCISO trend represents a huge business opportunity that cybersecurity service providers should explore as soon as possible if they want to remain competitive.

This survey aims to validate the significance of this trend, and to understand what is motivating the adoption of vCISO services by some companies or delaying their adoption by others, including perceived barriers such as additional headcount, time and investment – all of which can be avoided with a vCISO platform.

This research should be of interest to vCISO providers or potential providers who want to analyze how their current level of adoption measures up against the rest of the market, learn about the benefits and challenges of providing vCISO services, and access benchmarks around the activities, progress and plans of other vCISO providers.

Sources:

¹ [CISO Salaries](#), Glassdoor, June 2023

² [51 Small Business Cyber Attack Statistics 2023 \(And What You Can Do About Them\)](#), Astra Security, June 2023

³ [The State of SMB Cybersecurity in 2022](#), ConnectWise, May 2022

⁴ [vCISO: A Cybersecurity Leadership Career Path for Tech Pros](#), Dice, April 2023

Methodology

To get more insight into the growing vCISO trend, we commissioned a survey of 200 IT industry leaders to weigh in on how MSPs and MSSPs are leveraging this emerging, huge business opportunity to provide effective cybersecurity management for SMBs while creating a significant new revenue stream for themselves.

This report was administered online by Global Surveyz Research, an independent global research firm. The survey is based on responses from business owners, CEOs, CIOs, CISOs, COOs, vCISOs, Heads of Security and senior security consultants, in MSSP companies with 10+ employees and MSP companies with 50+ employees, across the US and Canada. These respondents represent North American service providers that are relatively security-oriented, unlike many of the very small MSPs that are focused solely on traditional IT services. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during June 2023. The average amount of time spent on the survey was 5 minutes and 57 seconds. The answers to most of the non-numerical questions were randomized, to prevent order bias in the answers.



Report Findings

Most MSPs and MSSPs Are Already Offering Components of a vCISO Solution

The concept of vCISO services is fairly new. Just a few years ago it wasn't being offered by MSPs and MSSPs at all, whereas now, 19% (almost one in five) are actively offering it as a solution. 26% of the larger service providers (100+ people) are leading the trend by offering these services, compared to only 13% of smaller companies (<100 people) (Figure 2).

Even among MSPs and MSSPs who aren't currently offering a dedicated vCISO solution, most already offer various components of vCISO services (Figure 1), most notably security awareness and training (31%), compliance monitoring and readiness (30%), and risk assessment (26%).

This means that they too have an opportunity to repackaging these components and offer them as a comprehensive vCISO service, creating a new recurring revenue stream and growing their business. In addition, they would be addressing the growing customer need for proactive cyber resilience, differentiating themselves from competitors, and making it easier to upsell additional products and services.

The barrier to leveraging this huge opportunity and offering full vCISO services is therefore not as formidable as some MSPs and MSSPs may think, since many of them already check the box for most vCISO responsibilities, and may only need to offer just a few more components to round off all of the essentials.

TIP: Check out [this eBook](#) to learn about the minimal requirements for providing vCISO services.

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

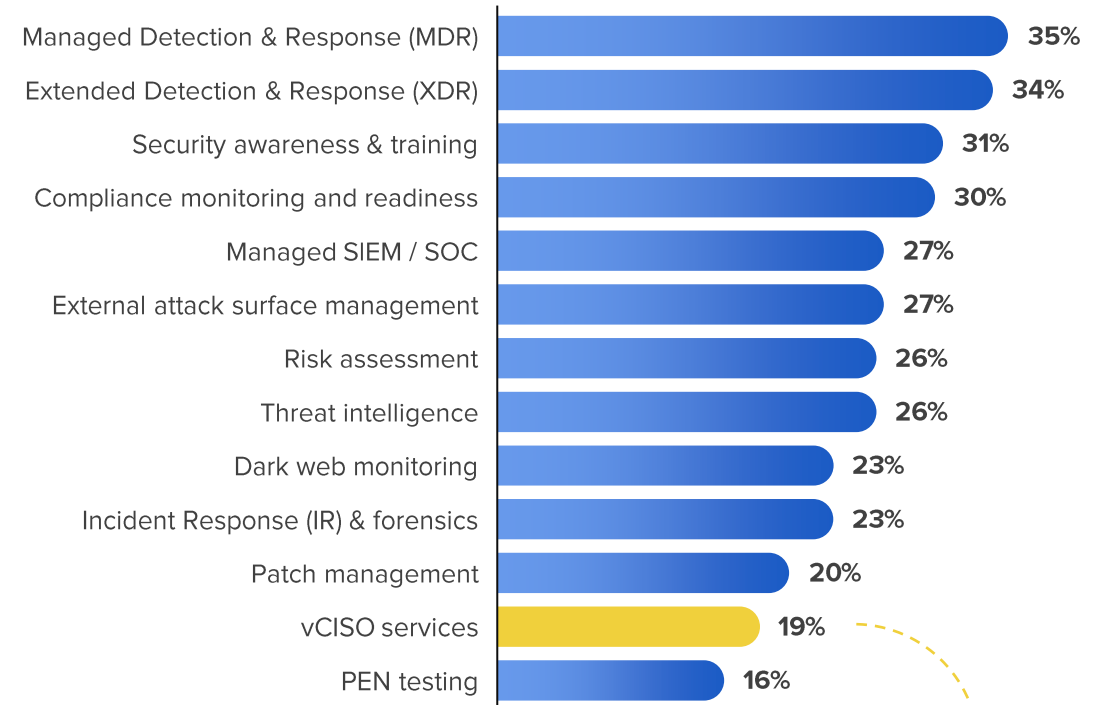


Figure 1: Products/Services Currently Offered by Companies

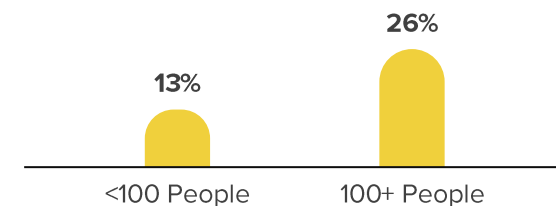


Figure 2: "vCISO Services", by Company Size

86% of Companies Currently Offer or Are Planning to Offer vCISO Services by the End of 2024

The vCISO trend is not going anywhere, with 86% of security-focused MSPs and MSSPs either currently offering vCISO services (19%) or planning to offer them by the end of 2024 (67%). In fact, by the end of 2024, it is anticipated that only 14% of security-focused MSPs and MSSPs will not be offering vCISO services.

Looking at the acceleration of this trend year by year, we found that only 5% of MSPs and MSSPs were offering vCISO services prior to 2022. Since then, the number of additional service providers offering this service has grown consistently, with 8% in 2022, 28% in 2023, and a projected 45% in 2024.

This confirms that the vCISO trend is decidedly 'hot', and those who fail to act on it well before the end of 2024 risk lagging behind competitors who will already have a vCISO offering in place.

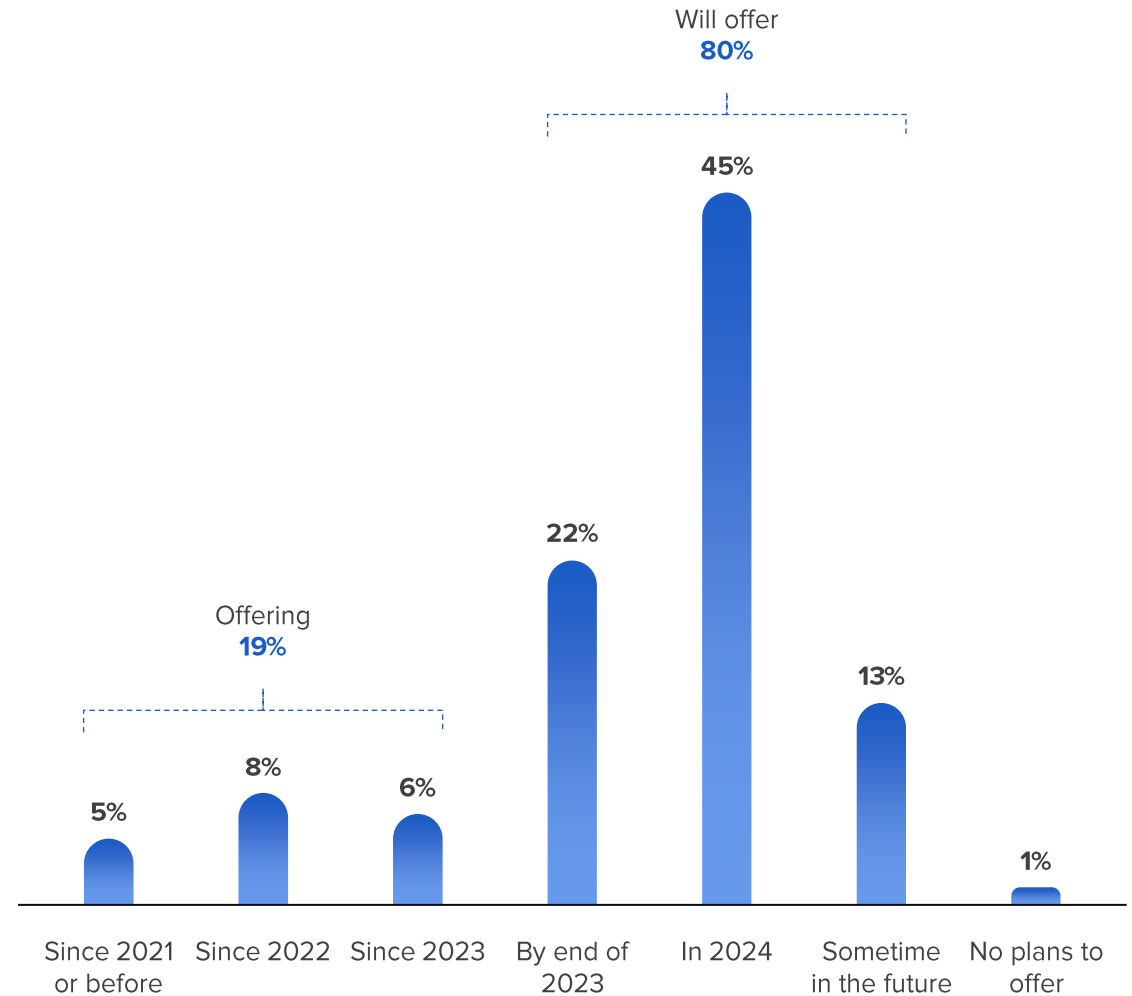


Figure 3: Timeline for Offering vCISO Services

Top Benefits of vCISO Services Validate Their Impact on Business Growth

Respondents rated the easy upsell of other products and services (44%), increased margins (43%), and improving customer security (42%) as their top benefits of adding vCISO services to an MSP/MSSP's offering. This is no surprise, given that **many MSPs and MSSPs – who are typically margin-driven – are moving towards security, because they see it as their path to growth.**

Also, the fact that most of the benefits for adding vCISO services to their MSP/MSSP's offering were rated by respondents fairly evenly – ranging between 33%-44% – suggests they understand vCISO services can improve their offering significantly across a wide range of areas rather than just one, making it an even more valuable addition to their stack.

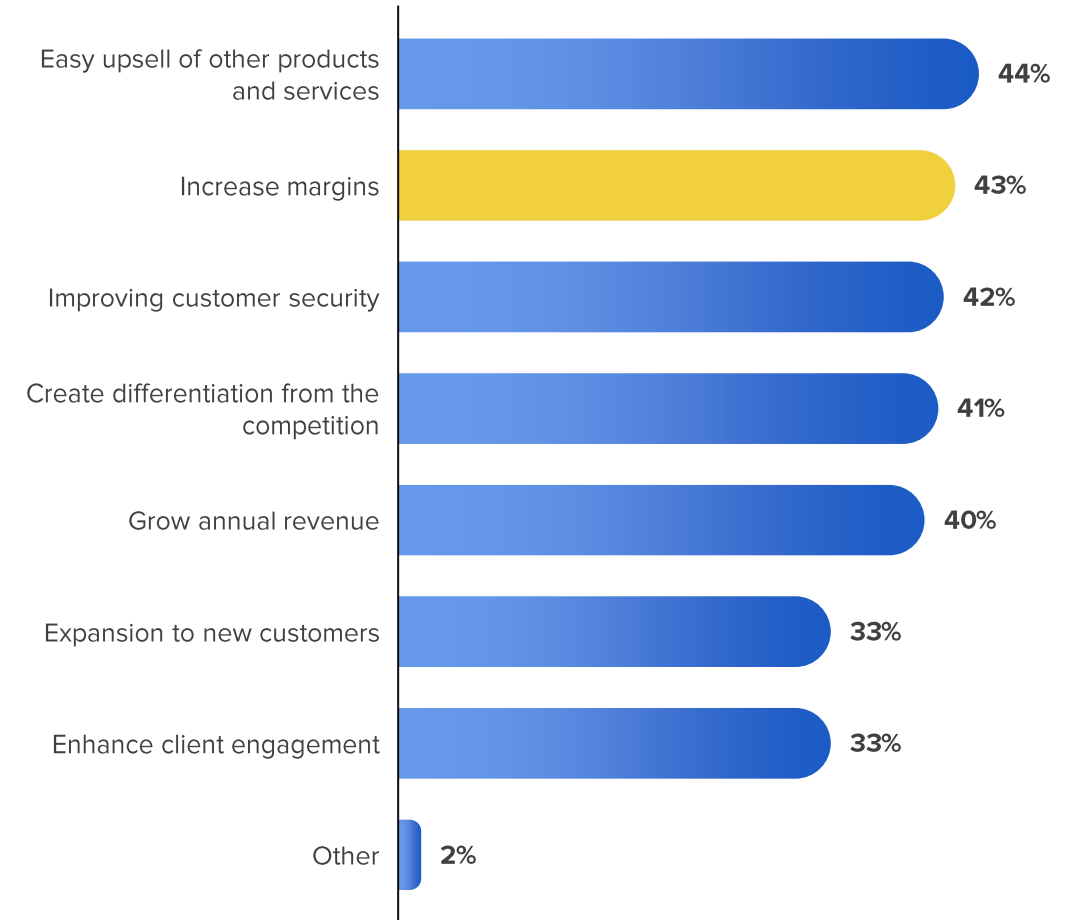


Figure 4: Top Benefits of Adding vCISO services to an MSP/MSSP's Offering

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

Top Benefits of vCISO Services Are Aligned with Main Strategic Focus Over the Next 12 Months

Respondents rated the expansion of their cybersecurity service offerings (39%), improving operational efficiency (36%) and improving profitability (32%) as their top strategic areas of focus for the next 12 months.

The choice of these leading areas of focus as their most pressing strategic goals – all of which relate to increasing profitability – is aligned with the benefits rated by MSPs and MSSPs as their top considerations for adding vCISO services to their offering, including increasing their margins (Figure 4).

This reinforces the urgency for service providers to add vCISO services to their services stack, because it can help them achieve both their margin targets and their cybersecurity targets. It also explains the rising vCISO trend.

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



Figure 5: Strategic Focuses for the Next 12 Months

Top Challenges in Providing vCISO Services

Although many MSPs and MSSPs believe that offering vCISO services will help them upsell products and services and increase margins (Figure 4) – they face a variety of challenges that pose a barrier to entry. The top challenges include limited security or compliance knowledge (40%), high initial investment (34%) and lack of skilled cybersecurity personnel (33%). Other challenges mentioned by respondents include limited customer maturity (31%), too many time-consuming tasks (30%), limited headcount (26%), and lack of technology (25%).

Many of these challenges are related to limited in-house expertise, which is one of the main barriers to entry.

Technology – leveraging AI, automation and cybersecurity knowledge – can help close this gap, and is arguably the primary catalyst for the booming adoption of vCISO platforms.

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

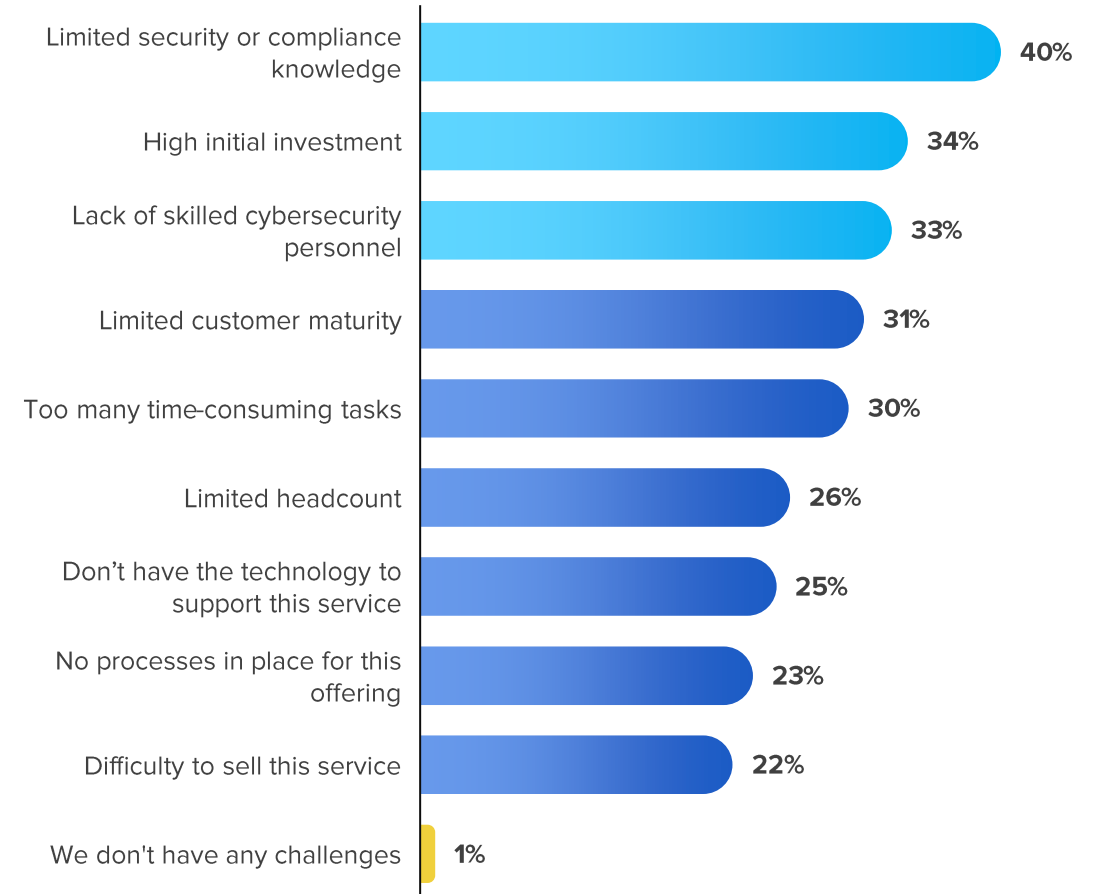


Figure 6: Top Challenges in Providing vCISO Services

91% of Companies Believe Offering vCISO Services Requires Hiring Cybersecurity Experts, while 63% Cannot Afford to Hire Them

As we saw in Figure 6, the top challenges in providing vCISO services relate to limited security and compliance knowledge and a lack of skilled cybersecurity personnel. When exploring this more deeply, the vast majority of the companies surveyed (91%) reported that growing their vCISO service or adding it to their offering would require growing their cybersecurity security team to “some” or “a great” extent (Figure 7).

But cybersecurity experts are both scarce and expensive, so unsurprisingly, 63% of respondents agreed to “some” or “a great” extent that their companies cannot afford hiring new cybersecurity experts (Figure 8).

This barrier to entry, however, is a myth. While it’s true that hiring cybersecurity professionals can be challenging, it’s now possible to provide vCISO services without recruiting expensive specialized personnel, by leveraging a vCISO platform that takes care of the heavy lifting through automating most of this work.

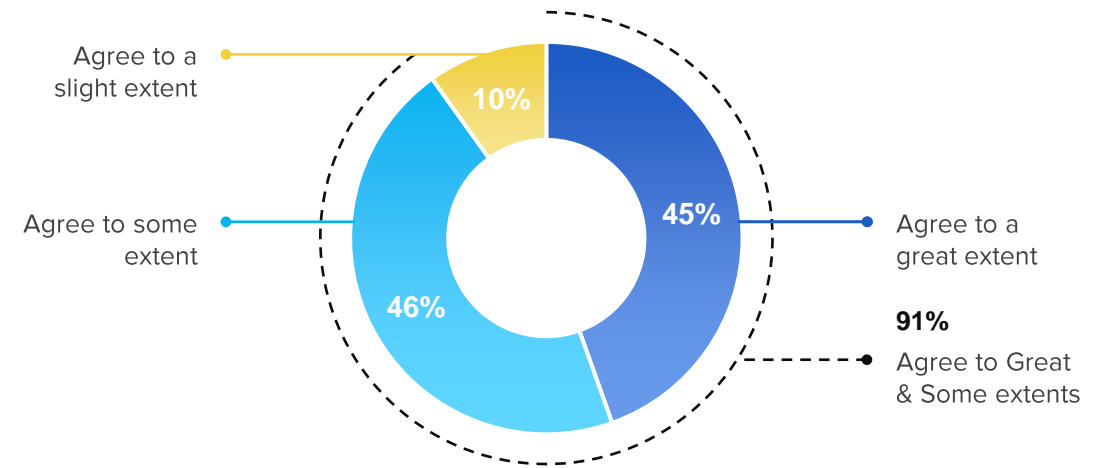


Figure 7: Growing our vCISO services or adding it to our offering requires growing our cybersecurity team

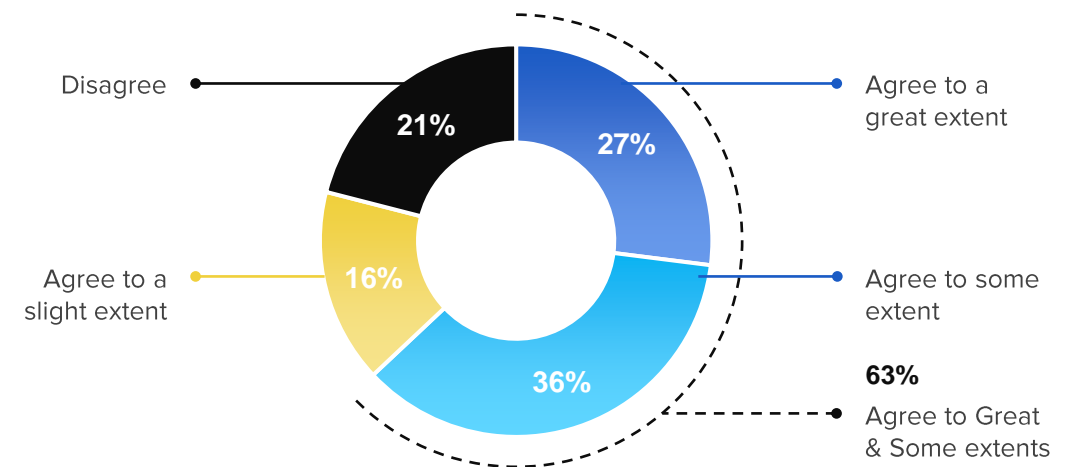


Figure 8: My company cannot afford hiring new cybersecurity experts

Most vCISO Tasks Are Time-Consuming

When it comes to the tasks generally performed by CISOs, they are typically all time-consuming, which means that a vCISO technological solution can make the entire process far more efficient – across the board.

We asked survey respondents to assess how many hours they spend on average on different vCISO-related tasks (by each time they deal with the task, per customer).

The top time-consuming tasks are periodical cybersecurity plan review (14.8 hours), building a remediation plan (14.7 hours), and creating security policies for a new customer (14.3 hours).

TIP: Technologies that automate these tasks can help MSPs and MSSPs optimize overall efficiency, reducing the time required to complete them by as much as 50%-80% and saving hundreds of work hours per month. [To learn more on these technologies, check out the top 6 vCISO platforms for 2023.](#)

#In Hours

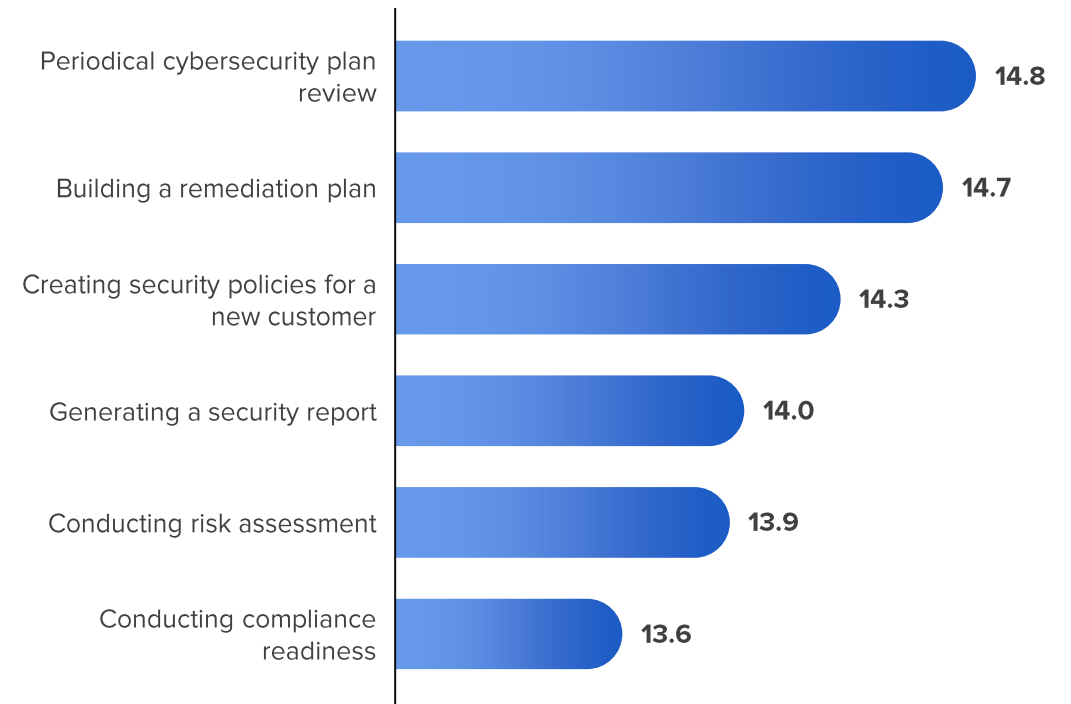


Figure 9: Average Hours Spent on Tasks



Demographics

Country of Residence



Figure 10: Country

Company Type, Company Size, Role and Seniority

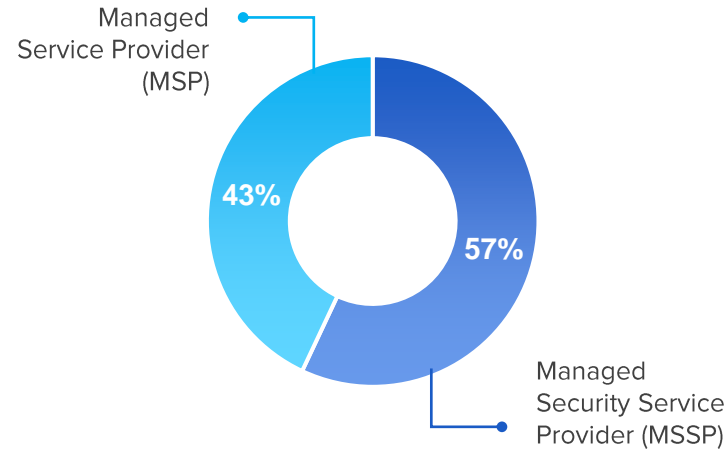


Figure 11: Company Type

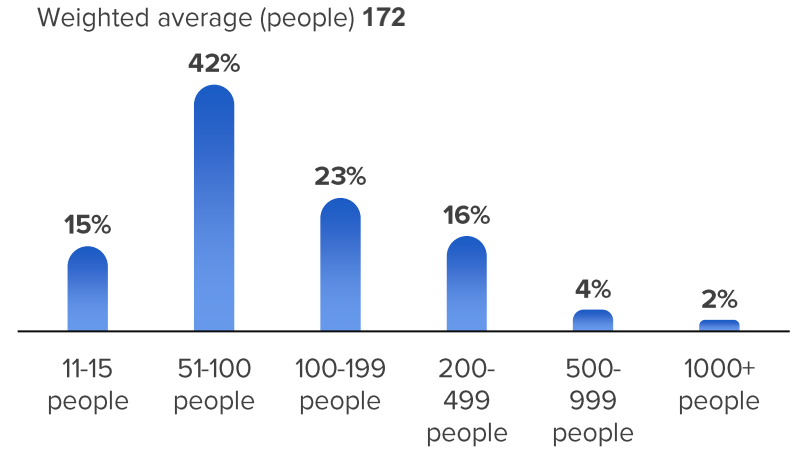


Figure 12: Company Size

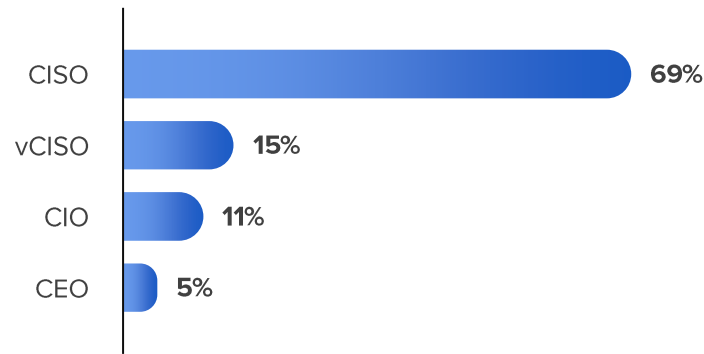


Figure 13: Role

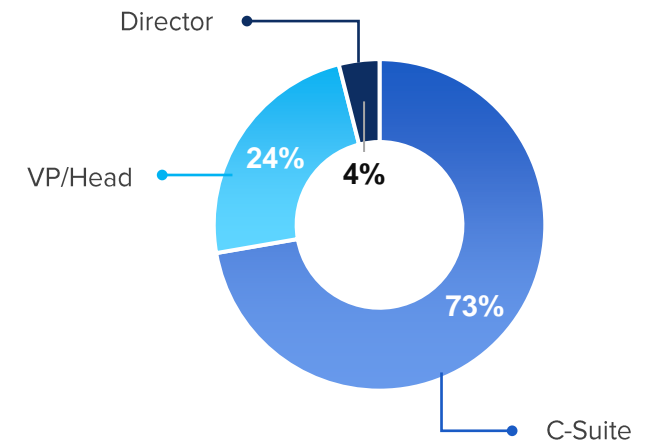


Figure 14: Job Seniority

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 platform streamlines the vCISO's 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.

Established in 2020 with the vision that every company deserves a CISO, and with a channel-only approach, Cynomi is trusted by more than 70 partners worldwide.

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

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

to learn more.

