cynomi

How MSPs, MSSPs, and Professional Service Providers Can Add vCISO Service at Scale

to Stand Out, Boost Recurring Revenues, and Reduce Churn – Without Scaling Their Own Resources

1 Introduction

Successful MSPs, MSSPs, and professional services firms often look for new services to sell to clients or new revenue streams to launch. Many see security services as a way to boost revenue and increase margins. But that often requires heavy investment in technology as well as the hiring of skilled and hard-to-find resources. As the cost of entry is high, it may be some time before profitability is realized.

Take the case of virtual Chief Information Security Officer (vCISO), which have recently grown in popularity. Understandably, some MSPs and MSSPs are considering the addition of vCISO services. But they tend to suffer from the same challenges as were outlined above – how to deliver them profitability without having to find people with the necessary skillsets or scale existing resources.

The purpose of this guide is to lay out what a CISO is, how vCISO services operate, how to bridge the skills gap, explain the difficulties many experience in delivering such services at scale, and lay out the steps to take to avoid these pitfalls and build a workable strategy for vCISO success. It includes an assessment of your own capabilities as well as tips on how to formulate a strategy and build a launch plan that enables you to succeed with vCISO services. And it details the massive potential for such services – a potential that is about to spill over into the SMB and Small and Midsize Enterprise (SME) level.

Let's begin!

2 What is a CISO?

Let's start by explaining what a CISO is, what a CISO does, and why this position has risen to prominence. Just as a ship needs a captain to stay afloat, large organizations, and technology intensive SMBs and SMEs need a CISO to plot the best course toward a secure future. To continue the ship analogy: A large ship has engineers, navigators, deck crew, service personnel, cooks, cleaners, officers, maintenance personnel, radar/sonar operators, radio operators, and many more roles. Each individually plays a vital part in keeping the ship afloat. But without coordination and leadership, they may inadvertently work against each other. In extreme cases, they may even take the vessel into the path of an iceberg. It takes a competent captain to steer the ship safely onward.

In this age of unprecedented levels of cyberattack, the CISO is the "captain of the cybersecurity ship." He or she is there to coordinate all security technologies, tactics, strategies, and processes to ensure the organization is protected currently and in the future. The CISO should not be immersed in the nuts and bolts of security logs, potential vulnerabilities, blocking phishing emails, and preventing data exfiltration. Rather, the CISO reviews summarized data about the overall security profile to assess risk and develop, implement, and enforce policy to protect critical systems, identities, and data while forwarding the overall goals of the business.

The CISO is typically involved in:

- Development and implementation of processes and systems used to prevent, detect and mitigate cyberattacks.
- Monitoring, evaluating, and managing overall cybersecurity and technology risk in coordination with business leaders.
- Setting an all-encompassing cybersecurity strategy that guides technology investment.
- Overseeing cyber governance, risk, and compliance processes.
- Reporting to top management and the board of directors.

As cybersecurity attacks, phishing scams, and ransomware outbreaks have ramped up in recent years, the role of the CISO has become even more critical. And with a large portion of the workforce operating remotely in many cases, the risk posture of organizations has shifted markedly. CISOs must constantly reassess risk and revise plans and policies to maintain compliance. This requires a solid knowledge of all applicable standards such as NIST, ISO, and PCi, as well as a firm grip on regulations such as HIPAA and GDPR.

It goes without saying that a CISO must be highly experienced in the world of security. Many have advanced degrees in IT and cybersecurity as well as certifications such as the Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), or Certified Information Security Manager (CISM).

3 Why vCISO Services Have Emerged

Two big reasons for the emergence of virtual CISO services are the scarcity of trained and experience resources, and the high salaries that CISOs command. A CIO or CISO earns an average of $170,000 in the US. With such a severe talent shortage going on within IT, these rates continue to climb. Bidding wars are commonplace for CISO-level skillsets.

States such as New York even require firms operating within regulated markets to fill the CISO position. Such requirements have pushed the average salary of a CISO in the greater New York City area beyond $270,000. That is well above the range of affordability for most firms – if a candidate can be found at all amidst an acute shortage of cybersecurity executive talent.

The security recruitment battleground has gotten so intense that CISOs, Chief Security Officers, and other high ranking security executives are changing jobs faster than ever. According to a study by CyLumena, their average tenure is between 18 and 26 months. Why? As the executives in charge of protecting corporate data, applications, systems, and end users, they have become essential assets to organizations. Hence, they get more unsolicited offers from headhunters than just about anyone in IT. LinkedIn messages flood in asking if they might consider a higher-paid job at X company. Attendance at an industry trade show is like sending a lamb among the wolves – offers of better-paid work abound. Due to hiring competition and other factors that impact attrition, many companies can no longer find or afford an IT security chief.

That's why various cybersecurity executive management firms, MSPs, and MSSPs have stepped up with solutions addressed at the CISO problem. They offer access to experienced and highly skilled security consultants. Instead of hiring a full-time CISO, organizations pay a subscription or retainer to gain access to expert cyber assistance in the form of a virtual CISO. These seasoned veteran executives "hold" the CISO position virtually, offering C-level assistance in devising and implementing strategies to prevent breaches, reduce risk, and mitigate the consequences of attacks.

They perform a vital role in building a comprehensive program that encompasses compliance and cybersecurity. They ensure that organizations put basic security measures in place to reduce the risk of a cyberattack as well as adequate safeguards to protect sensitive information.

Service providers are especially attracted to vCISO services due to their repeatability. Firms don't just need one-off help. They require a vCISO to keep track of their risk posture, security vulnerabilities, and to constantly revise the strategies and policies that will prevent cyber-devastation.

4 SMBs and SMEs: the Next Wave of vCISO Delivery

Fortune 500 companies often have a full-time CISO appointed – although holding onto them can be a challenge. When you get down to mid-size organizations, the number of CISOs dwindles significantly. Once you hit the small business level, they are virtually non-existent. Yet SMBs and SMEs need a CISO just as much as their larger competitors and partners. Why? Hackers have realized that they typically represent an easier target. They lack the resources, security expertise, and enterprise-class security tools that cybercriminals have to evade in larger organizations.

Accenture's Cost of Cybercrime Study found that nearly half of all cyber-attacks are now aimed at small businesses. Unfortunately, as few as 14% are prepared to defend themselves. Another study by the Ponemon Institute noted that 45% of SMBs believe their processes are ineffective at mitigating attacks, 66% have experienced an attack in the past year, and 69% have noticed that they are under more phishing and credential-related attacks than before. These are not just minor incidents where one person clicked on a phishing email and someone quickly removed a virus. Studies show that 40% of SMBs suffered eight or more hours of downtime after a breach.

The potential for MSPs and MSSPs becomes even more apparent when you consider that more than half of SMBs have no IT security experts in-house. Most MSPs have realized what many SMBs have yet to grasp – ransomware attacks could wipe them out if they don't take fast action. 85% of MSPs view ransomware as one of the biggest threats to their SMB clientele.

Those SMBs and SMEs that understand the security environment they now operate in have only a few options:

- Continue as before and hope for the best.
- Enter the CISO hiring arena and attempt to outbid the big boys.
- Seek out a provider offering vCISO services.

5 Why vCISO Services Are Difficult to Launch and Scale

In a climate like this, no wonder so many providers cast envious eyes towards the potentially lucrative vCISO space. Lack of trained CISO-class resources is the first barrier – one that prevents many from launching such services.

But others have leapt in and more than a few have achieved initial success. Margins were high and they could quickly procure multiple clients served by an in-house expert of two. But then they hit the wall. Scaling vCISO services proved difficult. Let's look at why vCISO services are so difficult to launch and scale:

A CISO is not some idle executive that sits with his or her feet on the desk, sipping coffee, and casually handing out the occasional instruction to IT personnel. It is a hands-on position and one that must constantly be on the alert, must stay on top of an ever-shifting risk profile, and must dig into the details of risk assessment and cybersecurity planning while staying on top of compliance and execution via top-notch project management skills. These actions are time-consuming.

Those offering vCISO services struggle to take on more than a few clients due to the following reasons:

- CISO duties demand expertise. A service provider may have one or two people internally who possess the know-how to operate at the C-level in security. But those tasks can't easily be handed off to other personnel. Any MSP doing so could endanger its reputation by using unqualified personnel to provide advice and strategy to customers.
- CISO duties are labor intensive. They need to work as swiftly and efficiently as the enemies they are up against. The more clients the MSP procures, the busier they get. Bottlenecks quickly occur and the quality of service suffers.
- Experienced cybersecurity personnel generally have other duties. MSPs and service providers must ensure their staff are well utilized to maintain acceptable margins. Few MSPs and MSSPs seeking to add vCISO services, then, will have the luxury of having cybersecurity veterans with free time on their hands. These experts are relied upon in other parts of the organization. The more vCISO clients that come on board, the more likely they are to neglect other vital duties.
- Risk assessments take time: The CISO conducts and regularly updates risk assessments to help the organization understand and document the existing cybersecurity risk posture. This is an essential step in finding out where things stand so that risk mitigation plans can be drawn up. There are various frameworks that CISOs may use for these assessments such as the NIST Risk Management Framework, the Operationally Critical Threat, Asset and Vulnerability evaluation (OCTAVE) Risk Assessment framework, the Factor Analysis of Information Risk (FAIR Risk), Threat Agent Risk Assessment (TARA), and others. Each provides a comprehensive evaluation of the overall IT environment from the viewpoint of security, vulnerability, and risk. These assessments address areas such as continually monitoring security controls in information systems, documenting changes to systems, conducting security impact analyses on any system changes, and reporting to top management on the security status of IT. These assessments absorb a large slice of any CISOs work week. Once a vCISO has a few clients, risk assessment leaves little time for anything else.
- Only when a thorough risk assessment is done can good planning be accomplished. The CISO develops and regularly revises policies to address issues uncovered in assessments and devise an actionable remediation plan with prioritized tasks. This plan must take into account every nuance of applicable regulations and standards to ensure compliance. Once again, this is a time-consuming activity.
- Personnel challenges: It may be cost-effective for an MSP or MSSP to give a couple of vCISO clients to a seasoned security professional that is already working for the organization. Once the workload goes beyond that scope, one possible solution is to hire in more expertise. But the expense of recruitment of CISO-caliber people will kill any hoped-for profitability and may even reduce margins further.

6 Assess Your Own Capabilities

Before laying out an effective way to solve the vCISO delivery conundrum, let's carefully assess your own current capabilities:

- Do mature security practices already exist or do they need to be developed before it would be possible to launch vCISO services? A good way to assess this is to impartially review how well you currently deal with cyber security issues.
- How happy are existing customers with your current cyber security procedures and capabilities?
- Who could run prospective vCISO services? This will require trained resources and must not detract from ongoing successful MSP service delivery efforts.
- Speak to your technical delivery personnel to find out how well they are coping with existing workloads. Are they already stretched?
- How many personnel are currently needed to deliver services and how many more are required to increase add new or improved services?
- What training and certifications have they completed and which ones are they most in need of?
- Based on this assessment, determine how well placed are you to consider launching new vCISO services or expanding them?

7 How to Add vCISO Services

In most cases, service providers are likely to find that they lack the skilled resources to add or further scale vCISO services. Here is what is required to achieve success as a vCISO provider:

- Security expertise: The provider needs at least one person who is knowledgeable and experienced in security and executive duties. Potential clients will want to know the credentials of this person before trusting the provider.
- If the provider is already delivering security or advanced IT services, such as person is likely to be present. If necessary, have the person complete a certification course that acknowledges their level of skill.
- If your skilled resources have existing duties, these duties should be turned over to others to enable this person to focus on vCISO matters.
- MSPs, MSSPs, and service providers should avoid taking on more than one or two clients initially. They need to gain experience at delivering vCISO services before offering them broadly.

These steps will help a provider begin delivery of vCISO services and achieve some success. Platforms exist that can assist MSPs with relatively little cybersecurity experience to bridge the vCISO skills gap and then scale such services effectively. This is achieved via the automation of the many manual aspects required of a vCISO to greatly reduce the workload. Only by doing so can you take on more clients without becoming overwhelmed.

Further, such a platform enables the provider to increase the quality of service available. Perhaps the person responsible for vCISO duties is not an expert in all facets of the position and lacks the years or executive experience typically required. Nevertheless, a good vCISO platform fills in the gaps to enable the delivery of high-quality services. Such software takes care of assessment and general planning automatically. It harnesses AI to take into account the many variables introduced by vulnerabilities, exploits, regulations, standards, and overall risk.

Its key elements are:

Automated software

It is not enough to direct veteran staffers to gaze into a crystal ball and somehow intuitively know where problems might lie and in which log the evidence of a breach or vulnerability will be revealed. There are just too many inputs and too many workloads to manage security threats in this outdated manner.

In the modern, cloud-based era, end-to-end automation is needed to take care of every facet of IT security. Automation must address assessment of risk, strategic planning of cybersecurity remediation in alignment with relevant standards and regulations, and management of the execution of those plans.

For MSPs and MSSPs in the vCISO arena, automation is a foundational element of effective scaling. To achieve acceptable levels of profitability, they must maximize the time spent delivering effective services. Every second absorbed in manually assessing risk or being bogged down in time-consuming processes cuts heavily into margins. The answer is to introduce as much automation as possible into risk assessment, strategic planning, the gathering of information about standards and regulations, and execution to lessen the burden on scarce internal resources.

Artificial Intelligence (AI)

Automation alone is not enough. AI is needed to bring the intelligence required to automate risk and compliance assessments, auto-generate tailored policies, and provide actional remediation plans with prioritized detailed tasks, task management tools, progress tracking and customer-facing reports.

This can only be accomplished by modelling AI algorithms on the best practices adopted by the world's best CISOs. Such an AI engine can continuously parse cyber profiles against relevant resources such as the NIST or ISO frameworks, industry standards and benchmarks, external threat intelligence tools, and compliance requirements.

8 How to Select the Right vCISO Platform Provider

AI-powered, automated vCISO platforms are emerging that are built from the ground up to continuously assess cybersecurity posture, automatically generate tailored policies and remediation plans with actionable tasks, and manage their execution. They help MSPs and MSSPs easily and quickly analyze and optimize clients' cyber posture, achieve and maintain compliance, and protect against data leaks, fraud, and ransomware. By automatically fusing cybersecurity knowledge and expertise with powerful scans and assessments, they create continuous end-to-end security posture optimization.

Features include:

- A single vCISO dashboard that provides a holistic view of each client's security posture and compliance readiness, and contains all you need to know for continuous improvement and compliance: cyber posture, risk management, tasks, compliance, policies, and benchmarks.
- Gap analysis: express-scan functions uncover critical vulnerabilities in externally visible IPs and URLs, ranging from email misconfigurations to unsafe use of encryption protocols.
- Real attacker's view: External vulnerability assessments include deep analysis of vulnerabilities and exploits for externally exposed assets (ports, protocols, encryption, website, web application, emails, DNS, and certifications).
- Tailor-made policies: automatically generate actionable policies specific for each client, based on all the internal and external intelligence to ensure an optimal personalized protection, covering everything from incident response to multi-site communications.
- Understand the impact of every action: AI-powered NIST-based assessments can be produced with security scores for specific threats, such as ransomware or website defacement. This enables the vCISO to see the criticality of changes and their effect on risk posture
- Customer-facing reporting: Demonstrate to your clients the remaining gaps, actions to take place and progress.

Cynomi, for example, provides a multitenant, vCISO platform that includes the above features. It enables service providers and consulting firms to easily set up or scale up vCISO services while reducing operational costs, professional knowledge gaps, and churn.

Cynomi builds a unique cyber profile for each client, based on questionnaires and scans, to then generate tailor-made cybersecurity policies on the fly. Based on benchmarks for every sector, vCISO service providers can demonstrate to their clients how they measure up on risk posture against their peers. The policies are then translated into actionable, prioritized tasks for execution, with impact analysis for each task.

vCISOs can immediately view the vulnerabilities their clients are exposed to refer to prioritized actions that lay out what to do next. This makes it easy for vCISOs to create a structured plan for compliance with policies that are mapped to any framework.

Cynomi lowers the dependence of the service provider in human CISO expertise. It enables providers to scale the amount of customers they can serve without hiring additional CISOs. It takes care of the manually intensive tasks that generate overload wherever the MSP or MSSP attempts to scale up. It arms the vCISO with a wealth of assessment data and automatically provides suggested actions that align with regulations and compliance requirements. This enables any service provider to not only serve more clients, but serve them better. The data and provided by Cynomi can be customized based on the priorities and know-how of the service provider. This transforms his or her work from the data gathering and planning function to execution. And even when it comes to execution, Cynomi helps by keeping track of tasks and timelines via project management features.

9

Formulate a Strategy and Launch Plan

Based on the findings from the above steps and assessments, a strategy must be developed on how you are going to launch and scale up services in a way that raises margins without placing undue strain on existing resources.

Here are some points to consider when making a strategy and a launch of expansion plan:

- Utilize the findings from earlier steps to develop a strategy that will enhance margins and facilitate scalability. This may include initial targets to address areas such as recruiting a security specialist, freeing up one of your key personnel to enable them to focus on vCISO services, providing more training to existing staff, or having someone complete security certification training. Until this step is accomplished, hold off on marketing or launch activities.
- Select a vCISO platform provider, deploy the software, and gain familiarity with it.
- Take on one or two vCISO clients and utilize the platform to deliver excellent vCISO services.
- Iron out any bugs until you are fully confident of your ability to deliver. This includes conferring with your platform provider to address any issues.
- Once your initial clients are satisfied with your ability to deliver vCISO services, develop a marketing strategy that encompasses how to upsell vCISO services to existing clients and how to develop new sales channels, particularly those that attract SMBs in desperate need of vCISO help.
- Define a set of metrics to measure business results. This might include leads generated, volume of website traffic, number of email responses, new subscriptions, revenue, and other parameters.
- Launch the service widely.
- Market the service forcefully to existing customers.
- Develop channels to find new markets and new customers
- Monitor results and use them to make adjustments in service delivery, support, or marketing to improve outcomes.
- When results and revenues justify it, step up vCISO service delivery and marketing, and invest more to further enhance the value of these services. This should include additional personnel for the new unit.