Apptega

Whitepaper

Unlocking Your Competitive Advantage

How Virtual CISO Services Can Help Your MSP Win More Business



Apptega

Traditionally, many companies left cybersecurity in the hands of their IT teams – generally, the people within the organization with the most technical experience. However, as the modern attack surface expands and the threat landscape becomes more complex, there is a growing and much-needed split developing between information technology (IT) teams and cybersecurity specialists.

Unfortunately, many organizations, especially small- and mid-sized businesses (SMBs), are struggling to recruit and retain skilled security personnel. And, furthermore, those lucky enough to find the right candidates often can't afford them, thus leaving critical positions unfilled. And to make matters more challenging, many organizations just don't have the allocated budgets, tools, or resources to tackle cybersecurity on their own

Although there are almost 5 million people around the world working in cybersecurity today, there remain between 3-4 million unfilled security professional roles.

With cybersecurity and compliance responsibilities now far greater than what the average IT team can handle, many organizations are looking for chief information security officers (CISOs) to manage these rapidly evolving programs. But, with limited resources and ongoing personnel challenges, many organizations instead lean on managed services providers (MSPs) and managed security services providers (MSSPs) for their expertise in the role of virtual CISOs (vCISOs).



Apptega

What is a vCISO?

Instead of hiring a full-time, on-site executive to manage cybersecurity, a vCISO is an outsourced security third-party that brings tactical and strategic security and operational experience to organizations that otherwise may never be able to afford or find the right person to hire. vCISOs generally work remotely and the positions are becoming increasingly popular as MSP and MSSP service offerings.

What Does a vCISO Do?

While some vCISOs manage operations remotely from a planning level, others are more involved, helping organizations implement cyber strategies such as program development, governance, and framework and control selection and implementation.

Among other responsibilities, a vCISO may also:

- Establish and measure key performance indicators (KPIs) and other metrics to monitor program performance and mature security practices.
- Serve as a liaison between your technical teams and your executives and key stakeholders.
- Ensure compliance and regulatory requirements are met.
- Develop cybersecurity policies and procedures.
- Provide training and education for your staff.
- Conduct risk assessments, risk management, and vulnerability assessments.
- Manage in-house security audits and serve as a liaison for third-party auditors.
- Complete the required documentation and ensure a single source of truth.
- Lead incident response and recovery.
- Align cybersecurity and compliance goals with the organization's goals and objectives.

According to Gartner, by 2025, nearly half of cybersecurity leaders will change jobs. Some 25% will move into different roles entirely because of multiple work-related stressors.

In addition to the expertise a vCISO brings to an organization, hiring a vCISO is typically significantly less expensive than hiring an on-staff CISO. According to a report from salary.com, the average CISO salary in the U.S. is about $230,000 a year. That doesn't include bonuses and benefits, which could add another $40,000 to $80,000 to that total.

Based on information shared by AT&T, the average cost of a vCISO is about 30-40% less than hiring a full-time CISO. And, since most vCISO services are paid with a base rate, organizations won't incur those additional benefits and bonus costs.

A Natural Fit for MSPs/MSSPs

According to the State of Cybersecurity Leadership and Readiness Report, 90% of large enterprises (5,000 or more employees) have an on-staff CISO or chief security officer (CSO), but there is a significant gap for SMBs. The report found that only 48% of mid-market businesses (100-5,000 employees) have a CISO compared to 36% of small businesses (fewer than 100 employees).

As SMBs continue to grapple with an onslaught of cyber-attacks – without the personnel or resources to effectively defend and respond – the need for vCISO services will continue to grow. Additionally, SMBs in highly regulated markets such as finance or healthcare can benefit from the added expertise of a vCISO to ensure compliance, especially as regulatory requirements change and more pop up across industries.

If you're an MSP or MSSP, you're likely already offering your clients IT and cybersecurity services, so expanding into vCISO offerings should be a natural fit for your business model. However, some of your clients may be hesitant to invest in cybersecurity and may not see the need for a vCISO because many SMBs have long had a mindset that they're not "big enough" to be a cyber-attack target. Others think that because they haven't *yet* experienced a cyber incident, their defenses are "good enough."

The reality is that today SMBs are just as much a target for threat actors as large businesses. While large businesses with on-staff CISOs are busy shoring up cyber defenses, attackers know SMBs are lagging behind and they're taking advantage of those weaknesses.

In 2021, for example, of the nearly 850,000 complaints the FBI's Internet Crime Complaint Center (IC3) received, a majority of those were small businesses. The Cyber Readiness Report 2022 found that companies with annual revenues between $100,000 and $500,000 can expect as many cyber-attacks now as companies earning $1 million and higher. The report also discovered that while cyber-attacks for large enterprises have decreased, attacks have increased for SMBs.

Small businesses with 10 or fewer employees have experienced a four-fold increase in cyber-attacks.

And even with that, a survey from CNBC and SurveyMonkey found that only about 37% of small business owners are concerned they will be a victim of a cyber-attack in the next 12 months and only 4% see cybersecurity as the biggest threat to their business.

.

Helping SMBs Connect With vCISO Benefits

As an MSP, you can help your SMB clients understand the actual risk cyber threats pose to their business and how your virtual CISO services can help them manage and mitigate those risks, all while saving them money and eliminating the need to hire additional staff.

But how do you get them to switch to a mindset they actually need your vCISO services? Here are a few talking points that may help bridge that gap:

- SMBs underestimate their actual cyber risk, even though they're experiencing an increase in attacks. Barracuda's Spear Phishing: Top Threats and Trends report says that the smaller the business, the more likely its employees will be a victim of an attack. Small businesses with 100 employees or less experience a 350% increase in social engineering attacks compared to those at large enterprises.
  - A vCISO can provide the education and training your staff needs to prevent those attacks from being successful.

- SMBs don't have the time, resources, skilled personnel, or money to build and manage an effective cybersecurity program.
  - A vCISO brings a wide range of expertise, knowledge, and experience to an organization without the expense of hiring a subject matter expert (SME). Since cybersecurity is one of your specialties, your vCISO can focus on security and compliance while your clients focus on what they do best — managing and scaling their business.

- Breach response and recovery are expensive, and in some cases could cause an SMB to cease operations altogether. The average cost of a data breach for small businesses with 500 or less employees is nearly $3 million.
  - A virtual CISO can build a cybersecurity strategy that decreases the likelihood of an attack and, by overseeing continuous risk management processes, more effectively stop an attack from spreading and doing greater damage.

- Technology and automation, such as a cybersecurity framework and control management platform, are essential to effectively decreasing cyber risk.
  - Your vCISO can use the power of Apptega to effectively manage frameworks, decrease risk, and meet compliance requirements with more insight, speed, and effectiveness than an SMB can do on its own.

- Cyber risk is business risk.
  - A vCISO can bridge the gap between the technical jargon of your security and compliance teams and your executives and key stakeholders by aligning security goals with business goals. A vCISO can also play a key role in helping your client's C-suite ensure operational resilience.

- Business is rapidly changing and so are customer demands and expectations.
  - A vCISO can help your clients keep pace by offering flexibility and scalability that can grow and evolve alongside their specific needs.

- There is no one-size-fits-all approach for cybersecurity. Because each business has different security and compliance needs, it can be challenging for SMBs to understand which frameworks and controls they need to implement and manage.
  - You can customize your vCISO offerings to meet your client's unique cybersecurity and compliance requirements.

Apptega

Gaining a Competitive Advantage

The Virtual CISO role is an emerging market, with estimates it could reach $10 billion by 2028. Beyond an increase in cyber events, other key drivers are pushing the market forward such as more complex cyber-attacks and increased costs of hiring in-house CISOs. There is also a growing awareness amongst some organizations that they need additional experience and support to protect their networks, systems, and data from cyber threats.

As clients' needs change alongside the threat landscape, it creates an opportunity for you to expand your services by having a vCISO ready to tackle their security challenges. You can also use your virtual CISO experience as a way to attract new clients and win a competitive advantage over your competitors by:

- Demonstrating the return on investment and value of your vCISO services (especially in terms of what it could cost a company if they don't have a CISO).
- Highlighting the experience and knowledge your vCISOs have, including awards and certifications.
- Explaining the benefits of using a vCISO compared to hiring a CISO or not having a CIO at all.
- Sharing customer success stories, especially if you have existing vCISO clients who have experienced a cyber event one of your vCISOs successfully managed.
- Showing clients that you (and they) can use framework management software to automate many of their security tasks and give them real-time insights into program performance without having to dig through stacks of paper or scroll through hundreds of cells on a spreadsheet.
- Demonstrating how using a platform like Apptega can help your clients save money on best practice, effective cybersecurity management processes.
- Marketing vCISO as a service offering and include it with a pricing package that makes it difficult for clients to pass up.
- Showing your clients that working with a vCISO on a monthly or similar retainer will keep their cybersecurity expenditures in check and they will always know what they're paying up front.
- Thinking outside of the box and instead of offering a standard checklist of cybersecurity management services, show your clients how you can serve their needs better than competitors because you can customize your vCISO offerings for them.

Apptega

How Apptega Can Help With vCISO Services

Like the SMBs you're serving, you may be wondering how you can meet a growing list of client needs, while simultaneously winning new business, with budget or personnel constraints yourself.

The good news is you don't have to go at it alone. Instead of having your vCISO bogged down in task management, Apptega can automate many core functions for you, for example, cross-walking security frameworks and controls, providing real-time compliance scoring, and even identifying where you have security gaps or issues, complete with best practice recommendations on how to address them. By automating many of these time-consuming and burdensome tasks, you can free up your vCISOs to focus more on strategy and operations.

With Apptega automation, your vCISOs can expand capacity and manage multiple client security programs at once, without fear of missing something important. One of Apptega's partners, Assessivate, has successfully done just that. Prior to implementing the Apptega platform, the company's vCISOs managed an average of two to four clients. With the power of Apptega, those vCISOs can now easily manage 10 or more clients effectively, with impressive customer satisfaction. Want to know how they're doing it? Read the Assessivate case study here.



Apptega

Here are some other ways Apptega can help with vCISO services:

- Quickly generate templated reports so IT and compliance teams always know how programs, frameworks, and controls are performing.
- Generate customized reports about program effectiveness related to business risk to establish KPIs and improve communication between your client's security team, executives, and key stakeholders.
- Assign roles and tasks and track status with automatic notifications to ensure no one drops the ball on responsibilities.
- Get alerts when a control or framework isn't functioning as intended.
- Get complete visibility into your client's entire environment so your vCISO can build confidence they've not overlooked any potential risk.
- Remove the guesswork and speed up response time by providing your vCISOs with best practice recommendations on how to resolve security or compliance issues.
- Keep each client's program documentation and evidence in one place so it's always accessible.
- Help clients prepare for audits with confidence by identifying and resolving potential issues before a real audit begins.
- Provide insight into each client's current security profile so your vCISO has the necessary information to strategize on maturing programs and reaching target profiles with clear timelines and metrics.
- Manage incident response and recovery.
- Conduct risk assessments and ongoing risk management.
- Continuously monitor security and compliance program activities.
- Utilize a marketplace designed to provide solutions and cyber insurance via Apptega Edge.

Scale to Meet Your Client's Security Needs

Trends driving strong demand for vCISO services will likely continue to increase. If you haven't already, now is the time to seize the business-growth opportunity to offer your clients virtual CISO services supported by Apptega. Together, you can help clients reduce the likelihood of a cyber-attack, decrease event impact, build confidence in recovery and response strategies, and do so while saving them (and you) time and money.

To learn more, visit apptega.com

Visit apptega.com