How Midsize Enterprise CIOs Can Engage a vCISO to Enhance Security

16 April 2025 - ID G00810801 - 7 min read

By: Paul Furtado, Fadeen Davis

Initiatives:Midsize Enterprise IT Leadership; Integrate Technology to Achieve Business Outcomes

> Midsize organizations grapple with a lack of dedicated security resources, leading to undue risk and regulatory challenges. Midsize enterprise CIOs can engage a virtual CISO to enhance their security practices and accelerate the implementation of a mature and defensible cybersecurity program.

Overview

Key Findings

- A cybersecurity program is complex and multifaceted, making it easy to accumulate scope creep and unnecessarily prolong the virtual chief information security officer (vCISO) engagement.
- The market of available vCISOs is growing with the result being varying levels of capabilities and competencies by different providers.
- Midsize enterprise CIOs often lack executive engagement on security matters, which risks limiting the reach of the vCISO to solely technical guidance.

Recommendations

Midsize enterprise CIOs looking to mature their security practices using a vCISO should:

- Clearly define the scope of the engagement by setting target outcomes and deliverables for organizational security defensibility.
- Maximize the value of the engagement by performing due diligence in the selection process not only of the organization, but also of the individual vCISO that will be aligned to their organization.

- Develop a clear engagement model for the vCISO role by establishing authority across the business to affect governance, risk and operational effectiveness.

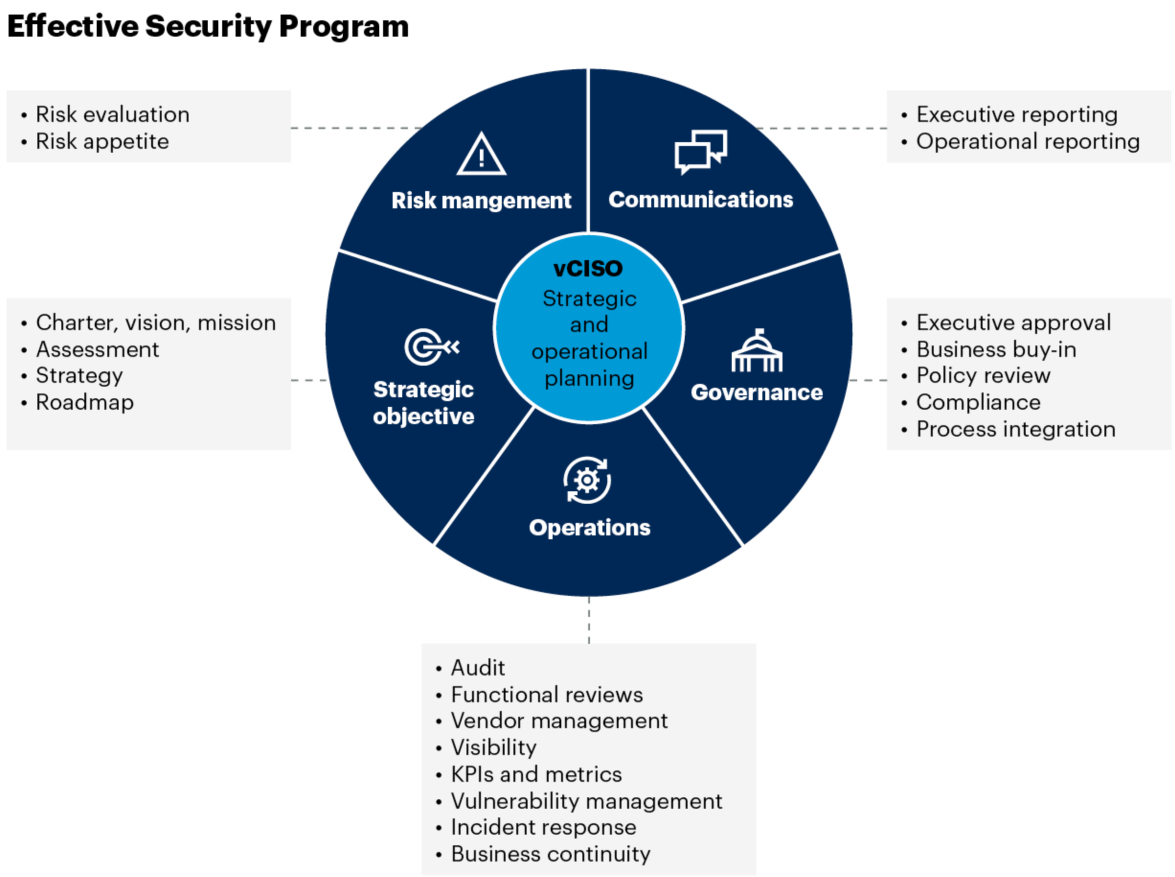
Introduction

According to a recent study of cyber insurance claims, over 98% of claims were submitted by midsize enterprises (MSE) over the last five-year period of the study. [1] This report demonstrates that attacks on MSEs are growing year over year, together with the costs involved in dealing with them. Additionally CEOs state that cybersecurity threats are impacting their business outlook and 85% of them say that cybersecurity is a critical component to achieving business growth. [2] This executive prioritization of cybersecurity means that midsize enterprise CIOs have to be able to demonstrate strategic and defensible levels of security for their organization.

There are several terms that are used synonymously to address this space. We see it represented as virtual CISO, vCISO, fractional CISO, and CISO as a service (CISOaaS). Although the names may vary, the service offerings are similar. For the purpose of this research, we will refer to these services as vCISO.

To be effective, a security program must be multifaceted and comprehensive, covering five key areas with several supporting elements (see Figure 1). All of these elements must be addressed both from a strategic perspective as well as a tactical and operational perspective, and the vCISO should be able to assist with all of them. This complexity requires a specific approach to the engagement to be successful.

Figure 1: Effective Security Program



Source: Gartner
vCISO = virtual chief information security officer
810801_C

The supplier market for vCISO services is increasing. In addition to traditional advisory and consulting firms, several managed security service providers (MSSPs) are expanding their offerings to include some type of vCISO service. Currently, 21% of security-focused MSSPs are offering vCISO services, and that number is expected to grow to 60% by the end of 2024. [3] That means that midsize enterprise CIOs will increasingly find different levels of capabilities in the market, which could lead to engaging with the wrong partner unless the proper due diligence is done.

Analysis

Develop a Clearly Defined Scope of Engagement

In order for a vCISO engagement to be successful, it is important to spend some time before engagement to determine “what good looks like.” Midsize enterprise CIOs need to have a clear vision as to what the outcome is that they want at the end of the engagement to avoid scope creep.

As shown in Figure 1, there are many moving parts to a security program. The reality is that every midsize enterprise CIO is already implementing certain parts of the program. The goal of using the vCISO is to uncover gaps within the existing program, mature areas that need work and provide assistance in implementing missing components.

Midsize enterprise CIOs utilizing vCISO services must:

- Determine the scope of the vCISO engagement. Ask questions such as:
    - Does the engagement of the vCISO include the entire security program?
    - Or is their engagement limited to specific areas (such as governance or incident response)?
- Be specific about any gap analysis activities to be executed. These activities could include:
    - Evaluation for compliance with a cybersecurity framework (such as National Institute of Standards and Technology [NIST], International Organization for Standardization [ISO] and Center for Internet Security [CIS])
    - Evaluation for compliance with regulatory activities (such as Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry Data Security Standard [PCI DSS], General Data Protection Regulation [GDPR] and Financial Industry Regulatory Authority [FINRA])

- Detail any expected deliverables and artifacts to be included in the engagement, such as:
    - Strategy
    - Policies and procedures
    - Dashboard and reports
    - Roadmaps
    - Risk register
    - Technical implementation

A vCISO should not be a permanent role. Our recommendation is that engagements should not exceed 12 months. A vCISO should be an accelerator toward the development of a mature security operating model. Upon contract termination, the vCISO should leave the organization in a position where the midsize enterprise CIO and their team can continue to follow their guidance and execute according to the roadmap that was delivered.

It is not uncommon to have some form of quarterly, semiannual or annual postengagement "check-in" to ensure the program is still meeting changing business requirements.

Perform Critical Due Diligence Activities

Selecting a vCISO partner is different from most other service procurement journeys. You are not only hiring a company to provide the service, but you are also hiring an individual. It is important to perform an effective due diligence of the experience and capabilities of the organization, and also of the individual, to ensure a fit for the organization.

Due diligence activities should include the following:

- **Organizational level**
    - *Experience:* Number of vCISO engagements they have successfully delivered in the last 24 to 36 months
    - *Capacity planning:* Number of vCISO professionals the company employs delivering the service and number of concurrent engagements they can deliver
    - *Deliverables:* Samples of required artifacts (such as policies, executive reports and risk assessments)
- **Individual level**
- *Experience:* Professional leadership experience, industry experience and regulatory knowledge

Develop Engagement Model and Functional Authority

For any security program to be effective, it cannot be an IT project. The vCISO needs to be treated as a strategic partner providing strategic business advice, not just technical and tactical IT guidance.

Work with senior executives to learn what kind of engagement senior leadership and the board will expect from the vCISO, and determine reporting requirements, key metrics and whether they want to engage with the person directly and at what frequency.

Successful executive engagement with leadership includes:

- Budget approval
- Operational and enforcement authority for security mandates
- Defining the reporting structure and cadence (including the ability to interact directly with senior leadership)
- Time investment by senior leadership — expect that interviews and on-on-one engagement will be required on a monthly (or regular) basis

---

It is critical to remember that a vCISO is not a risk transference project. The ultimate responsibility for cyber risk still lies with the organization and CIO.

Leveraging the services of a vCISO is not a mechanism to transfer the blame if something happens. You must ensure that the vCISO aligns with your organization's cybersecurity goals and values, and regularly review its performance, remaining actively involved in managing cyber risk. You can outsource the strategic and tactical effort, but you cannot outsource the responsibility and liability of cyber risk.

Evidence

[1] Cyber Claims Study: 2024 Report, NetDiligence.

[2] **2025 Gartner CEO and Senior Business Executive Survey.** This survey was conducted to examine CEO and senior business executive views on current business issues, as well as some areas of technology agenda impact. The survey was conducted from June 2024 through November 2024, with questions about the period from 2024 through 2026. One-quarter of the survey sample was collected from June through July 2024, and three-quarters was collected from October through November 2023. In total, 456 actively employed CEOs and other senior executive business leaders qualified and participated. The research was collected via 421 online surveys and 35 telephone interviews. The sample mix by role was CEOs (n = 303); CFOs (n = 95); COOs or other C-level executives (n = 39); and chairs, presidents or board directors (n = 19). The sample mix by location was North America (n = 194), Europe (n = 118), Asia/Pacific (n = 91), Latin America (n = 35), the Middle East (n = 15) and South Africa (n = 2). The sample mix by size was $50 million to less than $250 million (n = 32), $250 million to less than $1 billion (n = 122), $1 billion to less than $10 billion (n = 200) and $10 billion or more (n = 102). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] The State of the Virtual CISO 2024, Cynomi.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Tool: Midsize Enterprise Executive Security Dashboard

CISO Foundations: Cybersecurity Strategy Planning Best Practices

Quick Answer: CISO Foundations — How to Create a Cybersecurity Roadmap