5 KEY QUESTIONS

to Consider When Researching a vCISO Solution

SBS CyberSecurity

> **Organizations of every size rely on technology to operate, making it nearly impossible to function without it.**

If your organization suddenly lost access to all its technology today, could you still serve customers effectively?

For most, the answer is a clear no.

Organizations of every size rely on technology to operate, making it nearly impossible to function without it. Protecting and managing those investments — while securing confidential data, improving efficiencies, and maintaining a proactive security mindset — is essential to long-term success.

That's why appointing a chief information security officer (CISO) dedicated to overseeing information security and technology strategy is a critical step in evolving your organization's security posture.

Developing a proactive security mindset enables your team to make cyber decisions with agility and confidence. It also provides peace of mind knowing your organization has identified, assessed, and planned for potential information security risks.

OUTSOURCING: A TESTED SOLUTION TO A MODERN PROBLEM

Gartner forecasts that global spending on information security and risk management will grow 10.4% in 2025 to reach $213 billion, reflecting continued growth in cybersecurity investment.

Source: Gartner

Outsourcing to address an immediate need is a well-worn concept. Most recently, it's been applied to the information security industry through the virtual chief information security officer (vCISO) role.

Consistent breaches in information security, the exponential demand for security consulting, and a limited supply of qualified specialists all support the concept of outsourcing the key information security officer position as a viable option. However, understanding the intricacies of such an arrangement is vital to building a successful consultant partnership.

Reviewing the following five questions will provide your organization with the information needed to choose the best solution.

1

WHAT IS THE ROLE OF THE CISO?

A CISO wears many hats, but a major component of the role is developing an effective, dynamic information security program (ISP). A well-managed ISP empowers an organization to make informed security decisions and supports a proactive security mindset.

Though no two CISO job descriptions are exactly alike, core responsibilities often include:

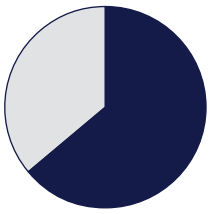
- **Developing and overseeing the information security program**
- **Addressing current cyber threats and identified vulnerabilities**
- **Managing a security team**
- **Ensuring effectiveness of the security awareness plan**
- **Developing risk assessments, policies, procedures, and plans**

A SUCCESSFUL CISO WILL HAVE:

- **Superb communication skills**
- **Deep knowledge of technology and security issues**
- **A strong understanding of the organization's business requirements**

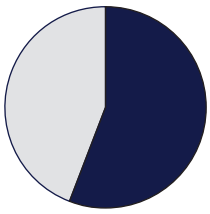
2

WHAT DO vCISO ARRANGEMENTS LOOK LIKE?



67%

of organizations report a shortage of dedicated cybersecurity staff.



58%

of organizations say cybersecurity staff shortages put their organization at risk.

In 2024, the global cybersecurity workforce gap reached

4.76M.

Source: ISC2

vCISO consulting arrangements come in many varieties and are used by organizations of all sizes and sectors. A vCISO may assist existing information security staff with specific assignments where additional expertise is needed, or they may take on several components — or even full management — of the ISP.

For larger vCISO consulting agreements, it is recommended that organizations maintain an internal information security coordinator to supervise consulting activities effectively.

Throughout these engagements, the consultant assists the coordinator in identifying the organization's areas of risk and determining the level of support needed, then follows up with a recommended work schedule. In addition, the consultant should work jointly with the coordinator to report significant findings to the board of directors or IT committee.

WHAT ARE THE BENEFITS OF HIRING A vCISO?

1

Avoid the pain and expense of the recruitment process.

Even with competitive compensation, recruiting a qualified CISO can take months and require a significant financial investment. With today's challenging job market and information security talent shortage, anticipate that the ideal candidate will be considering several opportunities. Organizations often spend weeks promoting their benefits and community appeal, only to lose a candidate to another offer with a larger package or shorter commute. Using a vCISO service provides immediate access to a team of cybersecurity experts, skipping the lengthy, costly, and uncertain recruitment process altogether.

2

Reduce stress and regulatory risk caused by IT staff turnover.

High turnover in the information security field can leave organizations scrambling to fill critical roles. The time and expense of recruitment, onboarding, and training can delay responses to pressing cybersecurity needs. A vCISO provides stability and continuity, bridging gaps during staff changes and reducing both operational and regulatory risk. With an experienced vCISO applying an established methodology, organizations can strengthen audit and examination outcomes while minimizing future disruption.

3

Gain expert-level knowledge instantly.

The skill set and knowledge base required for an effective information security program is constantly changing. vCISO consultants and advisors are not only certified professionals but also active practitioners who often perform similar roles with other clients in your industry. This exposure gives them broad insight into current threats, best practices, and proven strategies. When partnering with the right firm, the individual consultant is your main contact, but you can leverage a team of dedicated experts to augment their capabilities. vCISOs are trained, certified, and ready to help.

4

Manage the budget with predictable costs.

The information security job market is competitive, and turnover often occurs as salary and benefits expectations rise. Engaging a vCISO allows you to lock in labor costs for the term of the contract, creating a fixed budget line item. Another advantage is that you gain executive-level expertise without adding a full-time equivalent employee.

5

Establish a proactive information security mindset.

A vCISO can be a central part of your leadership team, providing insight to develop your organization's security culture. Depending on the provider, the consultant may participate in IT committee and board meetings. There's peace of mind in knowing decisions are made with information security factored in. A vCISO can also develop customized policies aligned with strategic objectives and drive a culture of proactive security.

6

Train staff to safeguard the organization's information.

vCISOs help strengthen employee understanding of cyber risk. This can include holding workshops on basic cybersecurity etiquette, sharing important security tips, ensuring employees use strong passwords, and training staff on multifactor authentication (MFA). Building awareness across all levels ensures security is a shared responsibility.

4

WHAT SHOULD BE CONSIDERED BEFORE CHOOSING A vCISO PROVIDER?

Before entering any outsourcing arrangement, due diligence should be performed to ensure the consulting firm has sufficient expertise and qualified staff to perform the intended work.

Since these arrangements take the form of a professional services contract, organizations should have confidence in the competence of the consulting firm and its team.

When negotiating a vCISO arrangement, consider both current and anticipated business needs and clearly define each party's responsibilities. Written contracts or service proposals should be reviewed to formalize these duties.

The following checklist highlights items that should be included in a vCISO proposal.

vCISO
Proposal Checklist

- Define expectations and responsibilities for both parties.
- Set the scope, frequency, and cost of work to be performed by the consulting firm.
- Arrange responsibilities for providing and receiving information, including how and how often senior management and the board of directors will be updated on contract status.
- Establish protocols for modifying the service contract, especially if significant issues arise requiring expanded consulting work.
- Affirm that all organizational information is kept confidential.
- Specify the locations of deliverables.
- Specify the retention period for deliverables.
- Determine the time frame for regulatory or audit review, ensuring examiners or auditors have full and timely access to deliverables and related work papers prepared by the consulting firm.
- Clarify whether the consulting firm will perform management functions, make management decisions, or act in a capacity equivalent to an employee or management member.
- Ensure the consulting firm complies with applicable professional and regulatory guidance.

As of 2024, cyberattacks are considered among the

TOP FIVE RISKS

to global stability.

Source: World Economic Forum

The average total cost of a data breach is

$4.88M.

Source: IBM

A ransomware attack will occur

EVERY TWO SECONDS BY 2031.

Source: Cybersecurity Ventures

5

WHAT QUESTIONS SHOULD WE ASK WHEN SELECTING A vCISO PARTNER?

There are many factors to consider when researching the best business to partner with for your vCISO agreement, which can make it difficult to know where to start.

The following questions provide a solid starting point for gathering the right information to make a well-informed decision.

Information-Gathering Questions

1 | When was your company founded?

2 | Who are the founders?

3 | Who is on the leadership team? What are their backgrounds?

4 | Is your company financially healthy? Will you provide financial statements?

5 | How do you differentiate yourself from competitors?

6 | Does your company have a proven platform to efficiently manage an ISP?

Note: This should include IT risk assessments, business continuity planning, business continuity risk assessments, vendor management, policies and procedures, and an action tracking and reporting process.

7 | Does your company perform criminal background checks for all employees?

8 | Over the next three years, how will your company's strategic plan change?

9 | Do you utilize exclusive contracts with specific vendors?

10 | Will you fill the vCISO position with one of your employees, or will you 1099 someone from another company?

11 | How many full-time equivalent employees does your company employ?

12 | Does your company utilize contractors/subcontractors or outsource any services being proposed?

13 | How many clients do you provide information security services to?

14 | Does your company have any awards or commendations in the last three years?

15 | Does your company have any experience in our industry?

16 | Will you provide a list of references in our industry that may be contacted?

17 | What are your top services per number of clients?

18 | What information security credentials and certifications does your staff hold?

19 | Do you have forensics specialists on staff?

20 | Will we be assigned a dedicated information security specialist?

21 | Does your company perform IT audits? If so, how are they managed?

22 | Does your company perform social engineering tests? If so, how are they managed?

23 | Does your company perform penetration tests? If so, how are they managed?

24 | Does your company have experience in red team testing?

25 | Does your company provide information security training?

26 | Has your company ever taken down a client's network accidentally?

27 | Can you share a sample incident response plan?

A COMPLETE SOLUTION

A well-designed vCISO approach allows organizations to manage or complement information security without overburdening current staff. This enables the organization to grow its business, stay ahead of threats, address annual compliance requirements, and meet — or even exceed — regulatory expectations.

As you contemplate hiring a vCISO, keep in mind that the security and protection of your organization's and customers' information ultimately remains your responsibility.

A skilled vCISO can guide you to make stronger cybersecurity decisions and take the right actions to protect your organization.

link.sbscyber.com/contact