5 KEY QUESTIONS

to Consider When Researching a vCISO Solution

SBS CyberSecurity

> Organizations of all shapes and sizes rely heavily on technology, making it almost impossible to live without.

If your organization threw out all of its technology today, could you still do business effectively while serving customers?

Most certainly, your answer is a resounding, “NO.”

Organizations of all shapes and sizes rely heavily on technology, making it almost impossible to live without. Protecting and managing your organization’s investments in technology, securing confidential information, increasing efficiencies, and embracing a proactive security mindset are crucial; especially when preparing and planning for future success.

That’s why appointing a chief information security officer (CISO) entirely dedicated to information security and technology is a strategic first step in evolving your security mindset.

Having an active security mindset with a proactive approach prepares your organization to make cyber decisions with agility and clarity. It also allows for better sleep knowing your institution has identified and planned for information security risks.

OUTSOURCING: A TESTED SOLUTION TO A MODERN PROBLEM

Gartner is forecasting worldwide spending on information security and risk management technology and services will grow

12.4% to reach

$150.4 billion.

That comes on top of a 6.4% increase in cybersecurity spending in 2020.

https://blog.barracuda.com/2021/05/24/gartner-security-spending-to-soar/

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

Consistent breaches in information security, the exponential demand for information security consulting, and a limited supply of qualified specialist 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 in 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 SUCCESSFUL CISO WILL HAVE:

- Superb communication skills
- Genuine knowledge of technology and security issues
- A well-founded understanding of the organization's business requirements

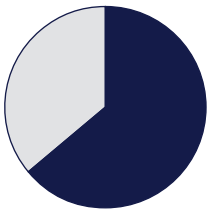
A CISO wears many hats, but a major component of the role is to develop an effective and dynamic information security program (ISP). A well-managed ISP empowers an organization to make more informed security decisions and supports a proactive security mindset.

Though no two CISO job descriptions are the same, CISO responsibilities may 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.**

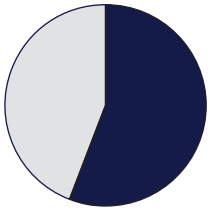
2

WHAT DO vCISO ARRANGEMENTS LOOK LIKE?



64%

of organizations report a shortage of dedicated cybersecurity staff.



56%

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

Worldwide cybersecurity workforce gap:

3.12M

vCISO consulting arrangements come in many varieties and are used by organizations of all sizes and sectors. A vCISO may be limited to assisting current information security staff with assignments in which they lack expertise. Other arrangements may call for the vCISO to perform several components or even full management of the ISP.

With larger vCISO consulting agreements, it is recommended for organizations to maintain an information security coordinator to adequately supervise consulting activities.

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

www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx

WHAT ARE THE BENEFITS OF HIRING A VCISO?

1

Avoid the pain and expense of the recruitment process.

Even when offering competitive compensation, recruiting a CISO may take an extended amount of time and a significant monetary investment to identify a potential candidate. With today's competitive job market and information security talent shortage, anticipate that the ideal candidate will be looking at several opportunities. Often, employers may spend weeks selling their organization's benefits and the community appeal, only for the candidate to choose another opportunity with a larger benefits package, signing bonus or salary, or less daily commute time. Using a vCISO service provides immediate access to a team of cybersecurity experts, thus skipping a potentially lengthy, costly, and risky recruitment process.

2

Reduce stress and regulatory risk created by IT employee turnover.

High turnover in the information security field can result in the scramble to find and onboard a replacement, creating additional costs for recruitment and training. Not to mention that a prolonged recruitment process and training period will delay the organization's response time to address critical cybersecurity needs. Enter the vCISO, who can provide the level of cybersecurity support and continuity your business needs. An experienced vCISO utilizing an established methodology can close the response gap and reduce the impact of future employee turnover and future information security gaps while improving examination and audit results.

3

Gain expert-level knowledge in an instant.

The skillset and knowledge base required for an effective information security program is constantly changing. Not only are vCISO consultants and advisors more apt to obtain and maintain professional credentials in the information security field, but these experts are also highly likely to be performing a similar role with other clients in your industry. That experience of working through a wide variety of situations from across the industry provides a consultant with an expansive skill set and a unique perspective of best practices and trends. On top of that, when partnering with the right firm, an individual consultant is likely your main contact, but you can leverage a team of dedicated experts to augment the talents of the individual assigned to your organization. vCISOs come pre-trained, pre-certified, and ready to help.

4

Better manage the budget with fixed costs.

The information security job market is competitive, and turnover occurs as salary and benefits expectations increase. Using a contracted vCISO allows the opportunity to fix the labor costs over the term of the contract, locking in a predictable budget line item. An additional benefit of outsourcing is that the organization is not adding a full-time equivalent employee to the employment roster.

5

Establish a proactive information security mindset.

The vCISO can be a central part of your leadership team and provide insight to develop the organization's information security culture. Contingent on the company you choose to partner with for a vCISO solution, the consultant may be available for your organization's IT committee and board meetings. There is peace of mind in knowing that decisions are being made with information security factored in. A vCISO can also create customized information security policies that align with your organization's strategic objectives and drive a culture of proactive security.

6

Train staff to safeguard the organization's information.

An important responsibility of a vCISO includes strengthening employee understanding of cyber risk. This can include holding workshops to establish basic cybersecurity etiquette, communicating important security tips, ensuring employees are using adequate passwords, and training employees on the proper use of multi-factor authentication (MFA).

4

WHAT SHOULD BE CONSIDERED BEFORE CHOOSING A VCISO PROVIDER?

Prior to entering any sort of outsourcing arrangement, due diligence should be performed to ensure that the consulting firm has sufficient expertise and several qualified staff members to perform the intended work.

Since arrangements are a professional services contract, organizations should be confident in the competence of their consulting firm and staff members.

When negotiating arrangements, organizations should carefully consider current and anticipated business needs while determining each party's responsibilities. To define these duties, written contracts or a proposal of services should be reviewed.

The following checklist covers the 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, such as the manner and frequency of reporting to senior management and the board of directors about the status of contract work.
- ✔ Establish the protocols for changing the terms of the service contract, especially for expansion of consulting work if significant issues are found.
- ✔ Affirm that any information pertaining to the organization must be kept confidential.
- ✔ Specify the locations of deliverables.
- ✔ Specify the period that deliverables will be maintained.
- ✔ Determine the time period that services provided by the consulting firm may be subject to regulatory or audit review and that examiners or auditors will be granted full and timely access to the deliverables and related work papers prepared by the consulting firm.
- ✔ Define whether the consulting firm will perform management functions, make management decisions, or act in a capacity equivalent to that of an employee or management member.
- ✔ Ensure the consulting firm will comply with applicable, professional, and regulatory guidance.

As of 2019, cyber-attacks are considered among the

TOP FIVE RISKS

to global stability.

(World Economic Forum)

A cyberattack occurs

EVERY 39 SECONDS.

(University of Maryland)

A business will fall victim to a ransomware attack

EVERY 11 SECONDS BY 2021.

(Herjavec Group)

https://www.varonis.com/blog/data-breach-statistics/

5

WHAT QUESTIONS SHOULD WE ASK WHEN SELECTING A VCISO PARTNER?

There are many things to consider when researching the best business to partner with for your vCISO agreement, making it difficult to know where to start.

The following questions provide a solid starting point in 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 information security program?
   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/sub-contractors 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, and how are they managed?
22. Does your company perform social engineering testing? 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 teaming a network?
25. Does your company provide information security training?
26. Has your company ever taken down a client's network accidentally?
27. Describe a sample incident response plan created by your company.

A COMPLETE SOLUTION

A well-designed vCISO approach will permit organizations to fulfill or complement information security management without burdening current staff. This will enable the organization to grow their business, stay ahead of threats, address annual compliance needs, and exceed regulatory expectations.

As you contemplate hiring a vCISO, keep in mind that the security and protection of your organization's and customer's information is still entirely up to you.

A good vCISO can truly guide you to make better cybersecurity decisions and do what is right to protect your organization.