ENTERPRISE
INTEGRATION

VCISO SERVICES

A White Paper on the Modern Role of CISOs

www.entint.com | Enterprise Integration | 866.802.3508

ENTERPRISE INTEGRATION

www.entint.com • 866-802-3508

VCISO SERVICES

A White Paper on the Modern Role of CISOs

Executive Summary

In an increasingly interconnected and digital world, organizations face a growing need for effective cybersecurity leadership and strategy. The role of a Chief Information Security Officer (CISO) has become paramount in safeguarding sensitive data, ensuring compliance, and managing cyber risks. However, many organizations lack the resources for a full-time, in-house CISO and find themselves at greater risk. This is where the concept of a Virtual Chief Information Security Officer (VCISO) has come into play. This white paper explores the evolving landscape of VCISO services, their benefits, and why organizations should consider incorporating them into their cybersecurity strategy.

Table of Contents

1. Introduction
2. What is a VCISO?
3. The Need for VCISO Services
4. Benefits of VCISO Services
5. Roles and Responsibilities of a VCISO
6. VCISO Service Delivery Models
7. Selecting the Right VCISO Provider
8. Case study
9. Conclusion

1. Introduction

Cybersecurity threats have grown in both volume and sophistication, making it more essential than ever for organizations to have a well-defined cybersecurity strategy. A VCISO is a flexible solution designed to provide expert cybersecurity leadership to organizations without the commitment and cost of a full-time, in-house CISO. This white paper will explore the world of VCISO services, addressing their importance, advantages, and how to select the right provider.

2. What is a VCISO?

A Virtual Chief Information Security Officer (VCISO) is a seasoned cybersecurity professional who offers part-time or fractional CISO services to organizations. The VCISO brings their high level of knowledge and experience to help organizations establish and maintain effective cybersecurity strategies. VCISO can be engaged on an ongoing basis or for specific projects, filling the gaps in an organization's cybersecurity leadership.

3. The Need for VCISO Services

Organizations of all sizes face cybersecurity threats and regulatory compliance requirements. Many organizations find themselves in one of the following situations that necessitate VCISO services:

- ✓ Resource Limitation

  Smaller and medium-sized organizations may lack the resources to employ a full-time CISO but still require high-level cybersecurity guidance.

- ✓ Temporary Expertise

  Organizations may need cybersecurity expertise for specific projects, such as implementing a new security framework, refreshing aspects of their security program, achieving compliance, or responding to a security incident.

✓ Knowledge Gap

Some organizations may have an IT team but lack in-house expertise to develop and maintain a robust cybersecurity strategy.

✓ Cost–Efficiency

Engaging a VCISO can be more cost-effective than hiring a full-time CISO, as it provides flexibility and expertise on demand.

4. Benefits of VCISO Services

Hiring a VCISO offers an organization many benefits, often even more than hiring a full-time CISO:

✓ Cost–Effective Expertise

Hiring a VCISO is a cost-effective way to access top-level cybersecurity expertise without the financial burden of a full-time employee. Organizations can engage a VCISO as needed, allowing for budget flexibility.

✓ Reduced Risk

VCISOs bring extensive cybersecurity experience, reducing an organization's vulnerability to security breaches. Their strategic guidance helps mitigate risks, protect data, and ensure compliance with industry standards and regulations.

✓ Scalability

VCISO services can be tailored to an organization's specific needs, whether it's for ongoing guidance or project-based work. This scalability ensures that an organization receives the right level of support when they need it most.

✓ Objectivity

An external VCISO can provide an objective viewpoint on an organization's cybersecurity posture, which can be invaluable in identifying and addressing weaknesses.

- ✓ Continuous Monitoring and Improvement

  VCISOs continually assess and enhance an organization's cybersecurity strategy, adapting to evolving threats and industry standards.

5. Roles and Responsibilities of a VCISO

A VCISO can take on various roles and responsibilities within an organization including:

- ✓ Developing Cybersecurity Strategy

  VCISOs' high level of knowledge and experience make them highly qualified to create and implement cybersecurity strategies aligned with organizations' goals and risk profiles.

- ✓ Implementing a Cybersecurity Framework

  Most VCISO's are well versed in multiple local and international information security and privacy frameworks. A VCISO can help a company select and implement, or update, an information security program based on a suitable framework.

- ✓ Risk Assessment

  VCISOs can help assess a company's risk by identifying vulnerabilities, evaluating risks, and developing mitigation strategies.

- ✓ Compliance Management

  VCISOs can ensure adherence to relevant industry regulations and standards.

- ✓ Security Incident Response

  Preparing for and responding to cybersecurity incidents, including breach management.

- ✓ Security Awareness Training

  A crucial role a VCISO can play is that of educator to staff on cybersecurity best practices.

- ✓ Vendor Risk Management

  Evaluating and managing cybersecurity risks posed by third-party vendors.

6. VCISO Service Delivery Models

VCISO services are delivered in various models:

- ✓ On–Demand

  The On-Demand Model allows organizations to engage a VCISO as needed, often for project-specific work.

- ✓ Part–Time

  The Part-Time Model gives companies consistent, ongoing VCISO support on a part-time basis, often a set number of days per week or month.

- ✓ Fractional CISO

  The Fractional Model allows for shared responsibility, where multiple organizations engage the same VCISO.

- ✓ Interim CISO

  The Interim Model places a temporary replacement for an absent or departing in-house CISO.

7. Selecting the Right VCISO Provider

Choosing the right VCISO provider is critical, and there are multiple factors to consider. Some of those criteria include:

- ✓ Experience and Expertise

  Assess the provider's experience, qualifications, and track record.

- ✓ Industry Knowledge

  Ensure the VCISO is familiar with your industry's specific cybersecurity challenges and regulations.

- ✓ Alignment

  Ensure the VCISO's approach aligns with your organization's culture and goals.

- ✓ References and Recommendations

  Seek recommendations and references from past clients of potential VCISO candidates.

8. Case Study

The below case study references an information security event experienced by a company who engaged Enterprise Integration VCISO services to help with incident response including compliance guidance, forensics, as well as technical remediation and clean up.

Use of Open-Source Intelligence and Social Engineering by Scammers to Make Paid Reservations for Travel.

This case study demonstrates how businesses are increasingly falling prey to clever fraud based on publicly available information that does not use sophisticated hacking techniques. Enterprise Integration has recently investigated multiple attacks that relied on strong social engineering techniques and non-technical means to scam companies for goods, services, or valuables.

In this instance, there were two distinct phases in which the attack was executed.

1. Reconnaissance Phase

   During the incident analysis, below is what Enterprise Integration discovered to be the information that was acquired and used by the scammers. The sequence may not be exact, but the below steps were taken to obtain information prior to execution of the attack:

- ✓ Review European company HQ website and determine foreign locations including location in the US
- ✓ Identified a Product Manager's name posted on the parent company's website including email and telephone number
- ✓ Obtain company's logistics email address (published on the parent company's website)
- ✓ Identified the company's travel agency
- ✓ Selected parent company's European HQ as the requestor
- ✓ Selected a US location as the payer and determined the name and contact information of an Executive Administrator in the US location

2. Building Trust and Execution of the Attack

- ✓ The Perpetrator, posing as a Product Manager from their organization European operations, initiated conversations with a US-based Executive Administrator. The administrator later stated that the caller knew detailed information about their company, and they could not fathom an outsider would have known so much internal information.
- ✓ The Perpetrator called a travel agent posing as the Product Manager and made flight reservations for five individuals for a meeting, requesting them to bill the US office and email the tickets to the logistics email address on the parent company's website.
- ✓ A few days later, the US Executive Administrator emails the European Product Manager requesting the name of the meeting to back bill the tickets to and receives a response from the Product Manager saying they were not aware of any specific tickets and asks for a copy to track them down.
- ✓ The Product Manager enquires internally within the European HQ if anyone was aware of the reservation.
- ✓ The reservation is determined to be a scam and reported to the FBI and other security agencies within the US.

Conclusion

Humans remain the weakest link whether in case of a socially engineered attack or even an attack that takes advantage of a technical vulnerability. Major security studies continue to say the same two things:

- ✓ First, users are the weakest security link, whether on purpose or by mistake.
- ✓ Second, insider attack poses the most serious threat to overall security.

What Can You Co About It?

- ✓ Provide Security Awareness Training to employees
- ✓ Review what you share publicly: website, newsletters, mass emails, etc.
- ✓ Build (off the band) verification processes within any process dealing with transfer of funds, intellectual property or any other valuable items
- ✓ Develop an incident response process
- ✓ Keep an updated list of government contacts in the incident response documentation
- ✓ Conduct routine Physical and Technical Vulnerability Assessments
- ✓ Ensure social engineering is included within Physical Assessments to test system robustness and employee knowledge

9. Conclusion

In a world where cyber threats continue to grow in complexity and frequency, the role of a CISO is indispensable. However, not all organizations can justify the cost of a full-time CISO. VCISO services provide a flexible, cost-effective solution for organizations seeking cybersecurity expertise, guidance, and risk management. By understanding the benefits, roles, and considerations outlined in this white paper, organizations can make informed decisions about integrating VCISO services into their cybersecurity strategies and fortifying their defense against cyber threats.