vCISO – Virtual Chief Information Security Officer

Service Definition

Table of Contents

1 INTRODUCTION

The internet is an inherently unsafe place, and determined actors look for weaknesses in an organization's defenses, from zero-day vulnerabilities to social engineering of employees. The threat landscape has evolved significantly. Protecting data and mitigating cybersecurity threats are some of the most prevalent concerns facing all businesses today. Proper measures and protection are vital to ensure that your business does not suffer.

One of the greatest risks to the critical infrastructure of businesses is not having a proper vision and direction for guiding resources on hand to address and minimize security issues. Without this, most organizations in the mid-enterprise market sector are not able to justify the added expense of hiring and retaining Security resources to safeguard in these areas. Moreover, standard services that result in checking a box for compliance purposes may provide audit fulfillment, but "Compliance" never equals "Secure."

Synoptek's Virtual Chief Information Security Officer Services (the "Services") provide your organization with the information security expertise and skills necessary to help your organization plan, define and execute an industry leading risk management strategy.

vCISO Platform (virtual chief information security officer) augments many of those information security management issues that are often overlooked. Our team of qualified information security experts become a virtual extension of our clients' leadership teams, providing best practices on how to manage and improve a company's risk posture.

2 SERVICE OFFERING

Most organizations can't afford a dedicated Chief Security Officer and resources to hire, train, and retain an IT Cyber Security Team, let alone, all of the tools needed to assure compliance and protection. The more sophisticated the threats, the more complex the response and skills of the responders. Synoptek's Virtual Chief Information Security Officer program helps each subscribing customer develop a tailored security framework to assess the required investment to reduce overall risk posture, while also addressing any regulatory compliance guidelines that an organization might be required to follow.

Key Features and Benefits:

- Cyber Security experience, expertise, total IT security dedication, and awareness
- "Vendor Preferred" perspective
- Focused on Cyber Security
- Help determine what Cyber Security services would contribute to the risk management strategy
- Established Cyber Security vendor relationships
- Creation and maintenance of a cyber risk management programs that is equal to or better than our competitors
- Compliance state assurance
- Knowledge of new regulations and industry changes

3 SOLUTION PURPOSE

The Service provides organizations with a Virtual Chief Information Security Officer with the executive leadership and skills to help plan, define and execute a security strategy tailored to meet its needs. The vCISO serves as an invaluable asset for your team to ensure the highest levels of security in terms of people, process, and technology.

4 HOW IT WORKS

The Service provides your company with a senior executive that is well versed in risk management and possesses a strong background in IT leadership. The vCISO engages with your organization on a regular basis to define and implement security, compliance, governance policies and procedures.

Get the benefit of having a dedicated, executive cyber security resource while saving time and financial investments:

- Flexible Consumption
  - As a service delivery model to fulfill short-term gaps in security governance needs with the operational scale to deliver long-term, ongoing security advisory services.
- Deliver Industry Expertise and Knowledge
  - Synoptek's vCISOs have consulting experience with environments across multiple industries that allow them to assist you using a tailored, reasoned approach
- Provide Instant Value
  - Synoptek's vCISOs' extensive IT Security experience permits them to quickly deliver risk management value
- Flexibility
  - Gain the ability to align your business with a solution that scales to your needs recognizing your existing security tools and budget constraints
- Vendor Neutrality
  - Benefit from a "vendor neutral" approach to technology; Synoptek's vCISOs make recommendations based on your needs, not the needs of technology vendors
- Adaptive, Not Reactive
  - Cyber Security threats are continually evolving and expanding. Synoptek's vCISOs hold a number of industry-recognized and highly valued certifications and maintain their skill sets to help clients address new threats

5 SCOPE OF SERVICES

The Service is inherently consultative and tailored to your security needs. As a baseline for any engagement, your subscription to vCISO should be used to evaluate and advise on the following:

Strategy & Operations

- Conduct initial planning, such as establishing timelines, document scope and confirming your objectives
- Align your IT security policies and risk management strategy with business objectives

- Define and develop key IT security policies for key needs such as: acceptable use, mobile devices, technology maintenance, incident response plans, remote access policies and process, business continuity and disaster recovery, etc.
- Security operations processes
- Third-party vendor security controls

Risk & Compliance

- Conduct an initial, limited-scope IT security audit and/or vulnerability assessment including social engineering
- Risk management - Determine level of acceptable risk, identifying critical assets and classifying information
- Compliance management

Threats & Protection
Establish, evaluate or test an existing threat assessment and remediation program to uncover intermediate threats and address the root cause of weaknesses and vulnerabilities:

- Vulnerability Assessment and remediation program development
- NIST-based Security Assessments (Security Diagnostic Level One)
- Additional CIS / ISO 27K Assessments are available at additional expense

Secured Design & Architecture
Help navigate complex environments, apply methodologies and incorporate leading industry security practices:

- Develop and architect systems, networks and infrastructure using security best-practices
- SIEM Log Analysis and Review (as part of SOC as a Service engagements)
- Provide network and security topological architecture diagrams
- SDLC (Software Development Life Cycle) security assessment and review

Incident Response
Establish, evaluate or test an Incident Response program to limit exposure and respond proactively and intelligently to incidents.

- Incident Response Program Development
- Incident Response Program Assessment
- Incident Response Readiness Exercise

In-house Security Briefings / Consultation
Tailor-made, target-oriented security Briefings for technical and non-technical personnel:

- General Security Awareness Training is also available as part of Synoptek's STAT Managed Security Services

6 SERVICE LIMITATIONS

Although this Service serves to improve the security of your data and/or assist in responding to security incidents, it will not eliminate your risk. Your organization retains ultimate responsibility for all risks and remediation of identified

conditions. Synoptek can provide support for such conditions via a *professional services* or *managed services* engagement which may incur additional expense.

The Service described is not synonymous with such roles as:

- Security Analyst
- Security Engineer
- Incident Response Team
- Security Operations

To the extent possible, the Service works to improve the maturity of your risk management program with an eye on industry standards, best practices, regulatory requirements, and the expressed cultural and policy requirements of your environment. Synoptek believes that the best approach to cyber security is a thoughtful approach to risk management, fostering a partnership with you to establish strong, defensible risk management hygiene. The Service cannot make assurances or guarantees with regard to audit events, regulatory compliance, or risks of compromise.

7 vCISO INTERACTION WITH OTHER SYNOPTEK SERVICES

This Service has the unique benefit of having direct access to the Managed Services catalog at Synoptek, as well as Synoptek's Professional Services team, which features an array of subject matters experts across knowledge areas ranging from networking to collaboration to application development and support to, of course, information security, governance, and risk management.

For customers of Synoptek's array of Managed Services, the vCISO will engage directly to evaluate existing services against best practices and is ready to advise regarding opportunities for instantiation of services to address gaps in your security and risk management programs. The vCISO will work with associated teams at Synoptek to provide oversight and guidance regarding service deployment strategy in manner consistent with your requirements and objectives.