BENEFITS OF USING A VIRTUAL CSO/CPO:

ORGANIZATIONS NEED TO ANTICIPATE AREAS OF IT RISK AND STRATEGIZE TO MANAGE IT AT THE EXECUTIVE LEVEL

A virtual CSO can bring both strategic and operational leadership on security to companies that can't afford a full-time person in the role.

Author: Shawn C Corrigan
President/Managing Partner
Interactive Security
www.intactsec.com
267.824.2500

Security is crucial in a technological environment, especially with all the complex risks that accompany the sheer amount of hardware and software used in public and private businesses each day. That's why cybersecurity is an absolute must.

Effective management of such complex environments is a requirement that will remain, making it necessary for both government and organizations to anticipate areas of risk, then strategize to manage it across all lines. Incidents and events that are considered a threat to any organization must be dealt with quickly and efficiently, hence the need to take a proactive stance to mitigate risk and create a secure atmosphere. This is where a virtual cybersecurity office, or CSO comes into play.

What Is a Virtual CSO?

Organizations are under a lot of pressure to keep their workplaces secure. Everyone from customers concerned about the safety of their information to regulators examining compliance will raise questions about the security of the information that comes in and goes out on a daily basis. A virtual CSO can help manage this risk, leaving organization leaders free to worry about other important areas of business.

A virtual CSO is a person who will visit an organization to implement security programs, answer board-level questions, and work with each department to improve overall security. This shows an organization is dedicated to ensuring security measures are in place at all times.

One of the myths surrounding cybersecurity is that a company needs to be a certain size or possess a particular amount of presence in the market before implementing cybersecurity is necessary. This simply isn't true. Both small and large organizations alike need to be secure.

Operating in a secure environment will enable organization leaders to concentrate on acquiring and assisting customers rather than worrying about the potential threat of hackers and compromised information. A virtual CSO will provide that security and demonstrate to potential customers the ability of organizations to handle risks.

The Role of the Virtual CSO

The virtual CSO will assess a company's needs, help develop best practices, create and assist in implementing a security program, and craft metrics for monitoring its effectiveness. Periodic testing will take place to ensure the program is working as it should.

Benefits of a Virtual CSO

Virtual CSOs save organization leaders money while placing subject matter experts at their fingertips. They also help implement time management measures that increase productivity and decrease the concern of security breaches.

Virtual CSOs are there when leaders need them, guiding teams, providing security reports, optimizing plans for budgets, assessing security, evaluating new security products, and assisting with incident responses.

Other tangible benefits of a virtual CSO include:

- A specialized and objective view of risk, security, and compliance

- The expertise of an experienced manager who will help the organization managers avoid costly mistakes

- Virtual and physical attendance at meetings

- Cybersecurity interface with partners, regulators, banks, and customers

- Evaluation and recommendation of security products and related technologies

Why Is Security Important?

Businesses retain sensitive information of all types, making it necessary to implement security measures that ensure it can't be placed into the wrong hands. Information such as payment details, health and medical, education, state and federal, and private company data all need to be protected.

A virtual CSO will provide high levels of protection to keep sensitive information confidential. CSO security services will include secure software development and implementation, system upgrades, network security, website updates, and mergers. Security will also be extended to client portals, so customers may enter and access information safely and without concern.

A virtual CSO will also provide the latest security news and assist with developing best practices and software recommendations. It will also be easier to track support tickets and keep up with support issues.

What Happens when An Environment Is Not Secure?

An environment that is not secure is open to data breaches that could prove detrimental to a business. Sensitive information that can be easily accessed can result in identity theft of customers and staff, lawsuits, and the mishandling of important data.

Taking proper security measures will protect both the business and customers, as well as strengthen trust between the members of the organization. Customers will be more apt to choose a secure organization where they feel their information will be safer.

Virtual CSOs Save Organizations Money

Virtual CSOs are cost-effective because they take the guesswork out of implementing security while saving organizations the expenses incurred by neglecting such measures. Turning the job over to someone who is well-versed in the industry will equate to a well-organized and secure system overall. A virtual CSO will advise organization leaders on the best ways to maintain security in the workplace across all platforms and will keep up with the latest technology trends.

Conclusion

Employing a virtual CSO will go a long way toward brand and organizational reputation. The technical infrastructure will remain uninterrupted and reliable, also protecting the financial and physical assets of the company.

Virtual CSOs also preserve the confidence of shareholders and customers, while creating a safer atmosphere for getting the job done. They will identify potential risks, prepare accordingly, and respond quickly, all while establishing the performance criteria necessary to reach positive results.

About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

*We pride ourselves on Making **IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*