Q: Our organization is contemplating hiring a virtual CISO. How does the role work and how do we ensure that it will be effective and meet business objectives?

A: A chief information security officer (CISO) is a C-level executive position primarily responsible for ensuring that the organization is capable of managing information security requirements. Information may pertain to the organization, its clients, its vendors and subcontractors. The CISO manages information security by establishing an information security framework, strategy, policy and standards within the organization. Given the high dependence on information technology, threat scenarios involving organizations being hacked for information that can be used to discredit the organization or that can be sold for nefarious purposes lead many organizations to find it increasingly necessary to appoint a CISO. However, organizations face challenges such as unavailability of the right skilled candidate, affordability of the CISO position and a potential candidate's understanding of business priorities when recruiting a CISO.

A CISO is expected to develop, establish and implement a framework to protect the enterprise's information assets by understanding enterprise objectives and communicating with various business functions and the senior management team. The CISO also leads and facilitates digital security governance for the organization based on policies and procedures, best practices, oversight, and monitoring of compliance. In addition, the CISO is responsible for building, promoting and endorsing a culture of security within the organization.[1]

A virtual CISO (vCISO) is an information security professional with experience in developing and implementing security frameworks, strategies and programs remotely.[2] Organizations may prefer to appoint a vCISO for various reasons, including:

- **Availability of qualified and experienced CISOs are limited**—Cybersecurity is an increasing priority for many organizations. The growing number of cyberattacks and data breaches combined with the escalating sophistication of attacks often necessitates a need for a skilled, experienced CISO role to manage information security. Many organizations are deploying state-of-the-art technology solutions with higher frequency, resulting in an increasing dependency on technology. Therefore, there is a need to focus on an organization's information security with a comprehensive set of controls and technologies, but CISO candidates checking all the required boxes for positions are not always available.
- **vCISOs are cost-effective**—Salaries for skilled and competent CISOs have been increasing due to high demand and limited availability of qualified candidates to fulfill this demand. A vCISO can be hired on a part-time basis according to an organization's requirements.
- **vCISOs are more experienced**—By the time a CISO is qualified enough to be hired as a vCISO, they are more than likely to have worked with many clients in diverse organizations.
- **vCISOs can work remotely**—vCISOs need not relocate to provide services onsite. The vCISO works as a consultant, working from almost anywhere, giving the organization exposure to more potential candidates. The recent pandemic has helped organizations adopt remote work cultures more seamlessly than ever before.
- **vCISOs are a requirement-based option**—Organizations can appoint vCISOs for a defined scope of work and determine payout per scope and services provided.

vCISOs can provide value to organizations by helping with a number of aspects of the overall information security program, including:

- Information security planning and management activities
- Organizational and management structure
- Initiatives affecting information practices
- Security risk management activities
- Evaluation of third parties with access to organizational data

SUNIL BAKSHI | CISA, CRISC, CISM, CGEIT, CDPSE, AMIIB, BS

Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

"There is a need to focus on an organization's information security with a comprehensive set of controls and technologies, but CISO candidates checking all the required boxes for positions are not always available."

- Coordination of audits by regulators or customers

Organizations facing these circumstances may consider hiring a vCISO:

- Small organizations that deal with sensitive information and question whether they can protect those sensitive data. A vCISO can help secure sensitive data.
- Small organizations that have resource constraints, particularly financial resources, can hire vCISOs for a limited period as cost-effective solutions.
- Organizations that require specific skills to protect special security requirements such as encrypting and tokenizing of privacy-related data using specialized tools or deploying data breach simulations using red and blue teams. In these situations, a vCISO with requisite skills may help deploy solutions. Other potential areas include defining needed security policies, classifying data, addressing procedures and policies to meet compliance objectives, performing risk assessments, and more. When the focus is not to fully develop and implement an information security program, but instead some subset of such a program, a vCISO is an excellent choice.
- Organizations that are considering appointing a CISO, however, hiring might not happen immediately. Experienced vCISOs can provide value in reviewing the current cybersecurity strategy and help select and transition to a new CISO.
- Organizations that have specific compliance requirements might engage a vCISO who specializes in a given compliance regulation to assist in developing a strategy and executing plans that meet the specific mandates.
- Organizations that need to realign cybersecurity investments can benefit from vCISOs who can help identify ways to more effectively and efficiently invest in cybersecurity initiatives.
- Organizations that are not sure what to do can benefit from engaging a vCISO to define road maps and develop frameworks for security, then identify and assemble the right internal team to implement security programs.

Endnotes

1 Putrus, R.; "The Role of the CISO and the Digital Security Landscape," *ISACA® Journal*, vol. 2, 2019, *https://www.isaca.org/archives*

2 Cavalancia, N.; "What Is a Virtual CISO?" AT&T Business, 9 November 2020, *https://cybersecurity.att.com/blogs/security-essentials/virtual-ciso-services-explained*