Improving Your Cybersecurity Strategy with a Virtual CISO

COMPUQUIP
CYBERSECURITY

Table Of Contents

Section I

Introduction

Today's organizations are more reliant upon their network infrastructure and systems than ever before. These networks host the mission-critical applications that allow them to deliver services to their customers and grow their business. They also manage the data that companies analyze for critical insights that inform their strategy as they work toward their objectives.

Protecting this infrastructure from risk with a comprehensive cybersecurity strategy is absolutely essential. Without the right security policies and controls in place, organizations leave themselves vulnerable to an array of cyberthreats, such as data breaches that expose sensitive customer information or ransomware that brings all operations screeching to a halt.

For many organizations, addressing cybersecurity issues begins with having the right person or team in place to develop and implement effective strategies for mitigating risk. Some of them decide to hire an in-house C-level executive known as a Chief Information Security Officer, or CISO. Other companies decide instead to turn to a virtual CISO solution that outsources many of the same responsibilities to a team of cybersecurity experts.

While there are many advantages to having a dedicated, internal CISO, partnering with an experienced virtual CISO provider offers most companies a more versatile and cost-effective solution to their cybersecurity challenges.

Section 2

What is a CISO?

A Chief Information Security Officer (CISO) is an individual in an organization that is charged with formulating the overall cybersecurity strategy—making sure that all of the necessary security measures have been taken, improving cybersecurity awareness, and creating contingency plans for when a disaster strikes. CISO duties can impact every process in an organization in some way—from the way employees use their emails, to which websites they can visit, to how they store important documents.

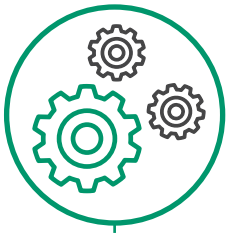
While similar to a CISSP (certified information systems security professional), there are some key differences. For example, CISO responsibilities typically involve determining the cybersecurity strategy of the organization as a whole because they are, by definition, a C-level executive. Meanwhile, CISSPs might provide recommendations or execute on said strategies, but are not usually responsible for creating the strategy. While a CISO will most likely hold a CISSP certification, not all CISSPs are CISOs (just like a CFO might be a certified accountant, while an accountant isn't necessarily a CFO).

Some of the key responsibilities of a CISO include:

Security Operations

The CISO is responsible for conducting real-time threat analysis of the organization's network. They should have a clear idea of the security status of firewalls, entry points, databases, and other network environments in order to respond quickly to any potential threats. Organizations also rely on CISOs to stay informed about the latest cyberthreats that could impact operations. When a data breach or other security incident occurs, the CISO is tasked with analyzing what went wrong and developing a plan to ensure it doesn't happen again.

What is a CISO?



Managing and Mitigating Risk

Risk can take a variety of forms when it comes to an organization's IT infrastructure. Data loss, fraud, natural disasters, system downtime, data breaches, insider threat, and human error all pose a threat to business operations. The CISO is often tasked with assessing the potential impact of these risks and implementing policies to reduce the likelihood that they'll occur and minimize their impact if they do happen.

Monitor Vendor Relationships and Compliance Status

Today's organizations face a number of compliance requirements when it comes to managing data. Failure to comply with these standards can expose a company to substantial liability, making it more important than ever to have someone tasked with continuously monitoring compliance status. In addition to developing the information security policies and controls needed to demonstrate adherence to compliance standards, CISOs must also monitor vendor relationships to ensure they are meeting the same requirements.

Provide IT Governance

Good cybersecurity regimes don't happen in a vacuum. Even the best-designed security policies and controls will be ineffective if they are not embraced by every level of the organization from the CEO on down to temporary staff. CISOs are responsible for promoting the importance of security programs and risk mitigation frameworks throughout the business to secure both the initial buy-in and ongoing adherence to established protocols.