CISO ToGo
Technology Risk Consulting

The Facts Can Not Be Denied – Virtual Chief Information Security Officer (vCISO) Best Option For Small to Mid-Sized Organizations

Organizations continue to face modern cyber-attacks such as ransomware threats and data breach incidents. In the wake of a non-stop onslaught from advanced hackers, it seems that no matter what defensive measures organizations put in place, cyber adversaries and malware authors are able to circumvent them.

But, cybercriminals are not only motivated to target high-profile enterprises; in fact, they actually tend to look at smaller and emerging businesses MORE, because they are assumed to be vulnerable targets. Most small and mid-sized organizations face a double-whammy when it comes to protecting corporate networks and having the foresight for tackling increasingly difficult mandates in governance, risk management and compliance (GRC) for long-term success. First, they struggle to commit larger budgets to finance evolved security fixes. Secondly, even if they are prepared to invest in modern defenses, they either suffer from a lack of in-house expertise or find it extremely difficult to source the right talent, such as a Chief Information Security Officer (CISO), from the market. This is because there's a serious shortage of skilled and experienced security professionals.

Findings from Verizon's latest Data Breach Investigation Report support this fact, as the research states that 43% of all breaches occur at small businesses. The same report also highlights that as high as 56% of data breaches take months or longer to become known, as this is largely due to the absence of the right kind of expertise.

Turning To A vCISO Is A Good & Pragmatic Option

At a time when regulatory guidelines are becoming more stringent than ever, with some recommending appointing a CISO, organizations must find a way to respond to modern cyber threats that are growing in scope and cost.

In doing this, the first daunting challenge lies in being able to manage and control all the potential weak points in the corporate IT network and end-user devices. Next, and this is where the real difficulty lies, is being able to do it with limited financial resources and in-house expertise — or even with the hired guns, for they are difficult to find. There is a pressing need to up the ante in cybersecurity to proactively combat a dangerous combination of mounting malware threats of increasing sophistication and a widening gap in the skills required to identify and combat them.

The time to consider useful alternatives such a hiring a vCISO is now, for it not only helps restore the confidence in an organization's IT security while correcting its risk posture, but it also would provide immense help to CIOs or IT managers in delivering a more streamlined and secure rollout of IT policies. Companies with either stretched financial resources or inadequate security expertise can discover a very meaningful use case in appointing a virtual chief information security officer (vCISO).

Among many of its obvious benefits include being able to move swiftly in the right direction to become compliant with emerging regulatory guidelines and plugging leaking holes to prevent data loss. What's more, contracting a vCISO isn't cost prohibitive like recruiting a full-time security expert. A vCISO comes with all the advantages that a full-time, seasoned CISO offers with their breadth of knowledge and security expertise. Further, a vCISO can help you conduct a quick assessment of existing IT programs and policies, ensuring your organization is able to make all the required changes to strengthen the security posture as demanded by the evolving cyberthreat landscape and regulatory climate.

Selecting A vCISO Goes Way Beyond A Makeshift Arrangement

For small to mid-size organizations looking to bring on a vCISO in a consulting capacity, here are some noteworthy traits you should consider before hiring:

- A vCISO should be able to articulate the inherent risks, educate management and explain available options in layman's terms that are jargon-free.
- Taking a page from former Intel CEO Andrew Grove's bestselling book, "Only the Paranoid Survive," the vCISO can never rest or rest assured. They should never be complacent but remain diligent (and, perhaps, even slightly paranoid).
- A vCISO should have a solid grasp on the fundamentals of IT security, ensuring daily tasks (like server security, patching, backups, and coding skills) are executed properly and consistently.
- A vCISO should strive to have good working relations with local law enforcement due to the inevitability of needing to report breach incidents (vCISOs need to respond urgently).
- A vCISO should have the talent to introduce creative approaches – especially at smaller organizations pinched by limited budgets. Focusing on employee training and ensuring two-factor authentication should be top of mind.
- A vCISO should possess good communication and collaboration skills to help win upper management buy-in to ensure that security remains a priority. Applying security protocols to existing products may boost sales while offering a competitive advantage.

The Bottom Line

Organizations that aim to seize emerging opportunities in digital transformation such as cloud, mobility, blockchain, the internet of things (IoT) and more — but fear legacy IT or poorly configured IT security environments as major bottlenecks — can think of vCISOs as strategists who are adaptive to their clients' needs and capable to help customers learn quickly to embrace disruptive technology with confidence and a well-planned road map.

Having trained and experienced cybersecurity professionals on staff can reduce an organization's risk to cyber-crimes exponentially. And when, **not if**, the organization does get attacked, an experienced cybersecurity pro can mitigate the problem and help to get the business back up and running quickly and efficiently ... **and that's where CISO ToGo can help**! To find out more information, check out our services listed on our website (www.CISO-ToGo.com).