vSEC

Driving Businesses Towards A Secure Digital Future

John Falck
Founding Partners

Securing cyberspace is unquestionably one of the most pressing issues confronting businesses today. The aggregate of businesses transforming digitally has grown exponentially in the past decade. While information technology has proved a blessing for many business sectors, it also created risks for the security of organizations' systems and digital data. These systems and data are the biggest asset for many companies, which makes their entire businesses vulnerable to cybercriminals and cyber-attacks.

To alleviate the vulnerabilities of various organizations, **vSEC LLC**—a Chicago-based cybersecurity consulting firm, leverages its business and security knowledge to help clients identify and better manage their cybersecurity priorities. Founding Partners Mike Phillips and John Falck first came up with the idea for the firm in 2017. Over the years, Mike, John, and their CISO (Chief Information Security Officers) peers had recognized that the demand for experienced CISOs greatly exceeded the supply, and that gap would continue to grow. Virtual CISO consulting allows CISOs to help many companies. Mike had over 25 years of experience as a Chief Information Security Officer whilst John had similar experience as a Business/Technology Executive before they jointly founded the firm with a goal to approach security needs in the context of business priorities.

MAXIMISING SECURITY

vSEC introduced its specialized cybersecurity consulting with a focus to provide executive-level guidance to businesses. Serving as a 'virtual CISO', or vCISO, vSEC helps firms assess their current security posture, to identify key risks, and to develop and execute a security strategy and roadmap that implements prioritized controls. These implementations involve a combination of policies, plans, and procedures, as well as supporting security tools. "*For many larger firms it is a complex process to understand what security tools they already own and how to get those (and other tools) integrated so they work as desired,*" asserts John.

vSEC clients are in the financial or financial-technology industries, healthcare, energy, regulatory compliance, and manufacturing. The company admires clients who are motivated to be secure rather than merely to document security compliance. It believes that security is not purely dependent on technology but does require adapting technology to securely support business activities. This business-focus approach to helping clients is the factor makes vSEC a frontrunner in the cybersecurity space. Its special skill is to combine cybersecurity and business understanding to help clients prioritize and implement a security program that is appropriate for their organization. This approach includes establishing security monitoring and reporting structures so executives and boards have insight into the effectiveness, risks and maturity of their security program.

As a virtual CISO business, vSEC states that while it performs some project-based contracts, the majority of clients hire it on a retainer basis, meeting on a fixed weekly schedule over multiple months to develop and execute a cybersecurity strategy and roadmap, whilst still being available to respond to urgent security questions as needed. vSEC is product and technology agnostic, so clients often approach it for advice when they want to review or select security tools or vended services.

> *"In turn, we have a network of CISOs and specialized security experts that we have known for years, whom we can introduce or ask for advice as needed,"* says John.

vSEC developed the security policies that a start-up required for rapid regulatory approval for their off-shore digital currency exchange and clearing business. Because of the timing of their launch, security policies and controls had to be developed before many people were hired or operations established. The client recognized that project requirements would change significantly, but also wanted to maintain the same regulatory approval and business launch dates for competitive reasons.

vSEC structured the project on a time-materials basis and coordinated with other security and technology specialists to ensure a quick response to changes during the project. Fortunately, with vSEC's combination of security, financial industry, and regulatory experience, it was able to anticipate and guide many project requirements. "*The project was a success - the security element of the regulatory review was perfect, and the business met its regulatory approval date,*" says John.

ADAPTION IS THE KEY TO BE SECURE

Cybersecurity is both professionally challenging and rewarding. "*As security consultants, our work makes people and companies safer, both decreasing the probability and impact of security problems and improving firms' abilities to detect and respond to security incidents that do occur,*" says John. As partners, they believe that security is not a problem to be solved once. "*Companies develop new business technologies over time, new threats emerge to attack those, and therefore new security controls are needed in response,*" explains Mike.

This constant evolution is exciting and requires a commitment to professional improvement and collaboration for CISOs and vCISOS to stay on top of their responsibilities. In the

cybersecurity sphere, companies constantly face external risks such as 'ransomware' and 'false payment' scams. However, the biggest security risks often are internal, coming from vulnerabilities in how companies operate, i.e., how they manage users, technology, and data. To address both external and internal risks, cybersecurity needs to offer protection through implementing and monitoring tools including anti-virus and firewall systems, and also needs operational controls such as limiting system access of users, restricting administrative system privileges, encrypting confidential data and testing backups.

As a member of the cybersecurity ecosystem, vSEC has established and maintained collaborative relationships with multiple specialist cybersecurity firms. It also has advisory relationships with some venture capital and private equity groups, which gives vSEC access to early-stage security companies and technologies. For example, one of its favourite start-ups developed a proprietary system to secure applications and data from attack even on compromised devices.

GUIDANCE IS ESSENTIAL

"*For too many firms, cybersecurity still receives a 'do the least required' priority,*" says John. vSEC anticipates a combination of pressures that may drive reluctant firms to improve and formalize their cybersecurity controls. Likely external forces include more companies reviewing the security policies and controls of their vendors, expansion and enforcement of privacy and data protection laws, and the insurance industry increasingly demanding proof of effective security controls as a condition for cyber-insurance. As another key factor, if boards and executives are held accountable for their firm's cybersecurity, as they are for supervising other business risks and controls, that may drive a large shift in executive attention to prioritize cybersecurity.

A jump in demand for cybersecurity likely will attract more security vendors leveraging and promoting next-generation security technology. vSEC expects it will take several years before the hype has settled and a few tools and services become well established. Through all of these transitions, vSEC expects that experienced cybersecurity advice will remain very valuable in helping companies understand and manage their security risks.

One worrisome issue for Mike and John is the potential professional dilution of the CISO and virtual CISO titles, and a resulting credibility risk to what is a relatively new profession. They both highlight estimates that there are only a couple thousand CISOs globally with 15 to 20+ years' experience, so many companies are chasing a small pool of cybersecurity experts. Since there is not a formal career path or accreditation to become a CISO, many individuals are getting such titles by taking the role. "Unfortunately, adding "and Security" to someone's job does not automatically give them necessary security experience," cautioned John. Some security service providers approach this expertise gap by offering standardized tools or reports, selling services that can be supported and replicated by relatively junior personnel. As a client focused business, Mike and John prefer to start with strategic level guidance and follow that by leading development and execution of cybersecurity plans. Hence, they expect vSEC's expertise providing advice to executives and boards that combines cybersecurity, business and operational experience will continue to be a competitive differentiator.

vSEC, LLC
Cyber Security Consulting

Mike Phillips
Founding Partners

"Companies develop new business technologies over time, new threats emerge to attack those, and therefore new security controls are needed in response," says John.