Your Trusted Advisor for Cyber Risk Management

Cybersecurity is no longer a technology problem left to the IT department. Cybersecurity strategy must be aligned with a business's overall strategy and requires focus and vision from a company's executive team. This the realm of the Chief Information Security Officer (CISO).

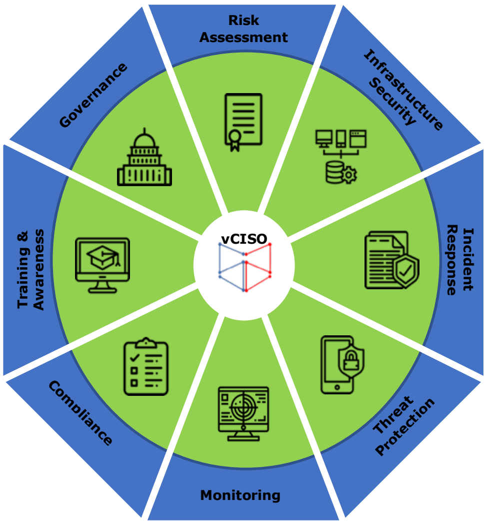
The role of the Chief Information Security Officer is an integral part of any leadership team, providing organizations with the needed expertise to manage the risk and threats they face. SSD Tech's Virtual Chief Information Security Officer (vCISO) program provides organizations with the executive cybersecurity leadership, decision-making support and operational capabilities necessary to address today's cybersecurity challenges. Our vCISO program is designed to seamlessly integrate into our client organization, making positive impacts in a short period of time.

54%
of SMBs believe they are too small to be attacked[1]

$369,000
is the average cost of a security breach for SMBs[2]

43%
of cyber-attacks target small and medium businesses[3]

Most small and mid-sized businesses believe they are safe from cyber-attacks, but the reality is quite contrary. SMBs are typically more vulnerable to breaches and hacks than larger organizations because they lack the security leadership, experienced personnel and financial resources to adequately protect sensitive data and systems. Further, SMBs are typically unaware of threats they face and how to apply best practices to reduce overall cyber-related risk. Our vCISO program provides an effective and affordable way to tackle current security challenges. Utilizing our vCISO management framework, we provide executive cybersecurity leadership and decision-making support customized to an organization's specific goals.



[1] *Ponemon 2018 State of Cybersecurity in Small & Medium Businesses (https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf)*

[2] *Hiscox Cyber Readiness Report 2019* (https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf)

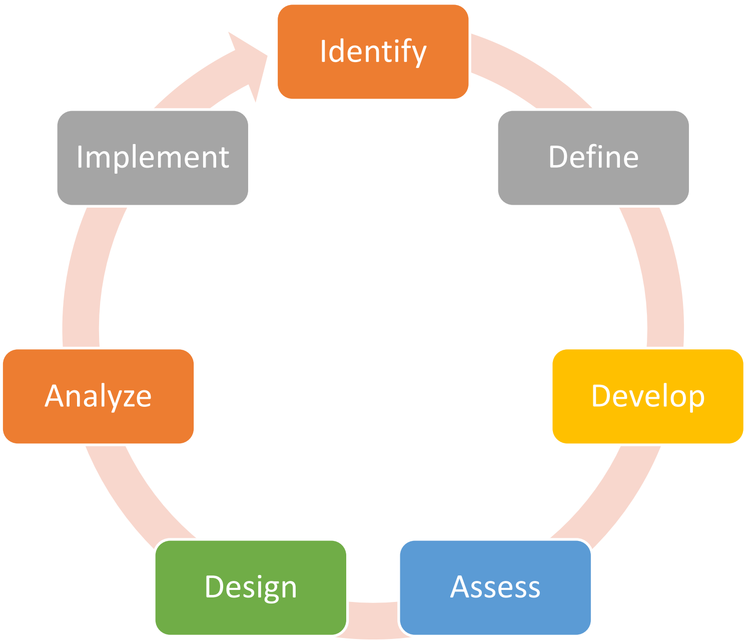
[3] *2019 Verizon Data Breach Report* (https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf)

SSDTECH

Virtual CISO

Our vCISO program utilizes industry standard frameworks, processes and strategies to meet organization-specific requirements. The vCISO program would:

Identify – Identify business strategies and objectives.
Define – Define systems and assets, regulatory requirements, and overall risk approach, including threats and vulnerabilities.
Develop – Develop an organizational profile by indicating what industry-standard cybersecurity controls, processes and procedures are to be followed/achieved.
Assess – Assess the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization
Design – Design the cybersecurity profile based on organizational goals, risk assessment and desired outcomes.
Analyze – Analyze the action plan to address gaps; reflecting upon mission drivers, costs & benefits, and risks.
Implement – Determine and implement actions as per the refined action plan to address the identified gaps and amend organizational current cybersecurity practices.



WHY YOUR BUSINESS MUST CONSIDER A vCISO

Digital Transformation – Digital transformation is inevitable as businesses strive to achieve competitive advantage. Security is a critical consideration as organizations transform their businesses.
Asset and Data Protection – It is proclaimed that data is the new oil. Organizations have to be vigilant while protecting this strategic asset. An effective approach to protect data and other assets must be implemented on a war-footing.
Risk Management and Governance – Properly managing cyber risk is a necessity for any organization it is no longer a luxury.
Regulatory Compliance – Many regulations require organizations have a qualified CISO in place.
Existential Threat – Cybersecurity is now a broad & complex problem that can wipe out the organization rather than just impacting a single department.

Our Approach

Risk Based

Whether meeting your obligations towards the regulators or the board and other key stakeholders, it all revolves around RISK.
And all we do is to reduce your risk. We have a proven track-record of assisting our clients manage their cyber-risk.

Managed

Measuring the progress of cybersecurity posture is an important part of compliance and ultimately peace of mind. Our approach includes all tools and data you need to measure progress. We will be your trusted partner throughout the process.

Continuous

Knowledge of all past, present and future threats and vulnerabilities is critical to the overall protection of your business. All our services are fully integrated, working together to provide a seamless cybersecurity program.

Realistic

Time, budgets, skilled resources are always constraint when addressing the cybersecurity challenges of your business. Our experienced consultants have lived through these challenges themselves, therefore we passionately offer only practical security and no fantasies.