SSDTECH

Cybersecurity Services

Your Trusted Advisor for Cyber Risk Management

No data is completely safe. Cyber-attacks on companies and individuals are on the rise and growing, not only in number but also in ferocity. While you may like to remain in a false sense of security thinking you have taken all the precautionary steps to prevent an attack, the uncomfortable truth is that no individual, company, or country is secure from cyber-criminals.

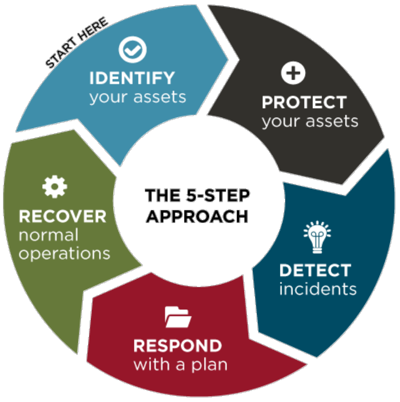
Information security can no longer be left exclusively to IT specialists. Improving and increasing information security practices and identifying suspicious activity is everyone's responsibility, from the boardroom executive to the bottom most employee.

62%
of SMBs lack a defined cyber- risk management strategy[1]

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

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

All businesses, no matter the size, need to ensure everyone involved in the company is up to date on the latest cyber-threats and the best methods for protecting company data and systems.



No longer can businesses assume cyber-crime cannot or will not happen to them. Implementing a strategic cybersecurity plan to assess and mitigate cyber-risk has become a necessity for all businesses. This is exactly like any other strategic efforts or operations in other critical areas of business.

Cybersecurity is NOT only an IT problem, but a company-wide issue that requires a disciplined and regimented approach to protecting data, assets and systems. Effective cybersecurity practices don’t end at the firewall or the computers anti-virus software, but must include strategic planning, training, governance and operations.

[1] *Vistage Cyberthreats and Solutions for Small and Midsize Businesses* (https://www.vistage.com/wp-content/uploads/2018/04/Cybersecurity-Research-Note.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

Cybersecurity Services

As part of our mission of securing our clients' digital universe, we strive to make security a strategic and measurable part of their organization. As a trusted security advisor, we will assess the existing information security programs and develop, implement and manage customized information security protocols through the following services:

Governance

Cyber-threats have grown so large that their consequences can significantly impact a company's bottom line. As a result, cybersecurity and data privacy are now executive-level governance concerns.

Risk Assessment

Everyone knows that there's some level of risk involved when it comes to a company's critical and secure data, information assets, and facilities. But how do you quantify and mitigate this cybersecurity risk?

Compliance

Program design and implementation of a cybersecurity framework (PCI DSS, ISO27001, the NIST Cybersecurity Framework, etc.) that ensures effective risk, compliance and resource management.

Threat Protection

The foundation to a solid security program is quality security technology. Advanced security solution(s) which will protect from attacks and provide visibility into malicious activity.

vCISO

Whether you need high-level strategy, or deep technical expertise, our vCISO service will deliver the expertise and experience in all areas of cybersecurity. Our vCISO program is tailored to meet the business objectives of the client.

Continuous Monitoring

Often overlooked and potentially the most important piece of a comprehensive security program is the continuous monitoring for threat activity and new vulnerabilities.

Awareness Trainings

A comprehensive program to educate and test the weakest link in the security posture – Human Resources. Executed over a period of time allowing employees to recognize phishing attacks and other ways they can improve security in the organization through improved interactions.

Application Security

Our application security program focuses on making your apps more secure by finding, fixing, and enhancing your apps. The sooner we find and fix security issues in the software development process, the safer your apps will be.

Incident Response

Our security incident response service investigates the attacks, contains the impact, takes immediate remediation actions by collaborating with your in- house resources, and finally assisting in restoration of data and systems to a protected state.

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.