HARBOR TECHNOLOGY GROUP

Cybersecurity as a Business Enabler

Why your SMB needs a Virtual CISO

Cybersecurity is no longer a technology problem that should be left to the IT staff. Cybersecurity challenges coupled with a business's overall goals and objectives must be considered in tandem requiring focus and vision from a company's executive team. This is 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.

Harbor Technology Group'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. Harbor's vCISO is designed to seamlessly integrate into your organization, making positive impacts in a short period of time.

76%

of SMBs have reported that they have been impacted by at least one cyber attack in 2021.

$382,000

is the estimated loss for medium sized business that is the victim of a cyber attack.

60%

of SMBs closed their businesses within 6 months of a data breach

More Information:
www.harbortg.com

Contact Phone:
(609) 429-0842

CYBERSECURITY
A BUSINESS PROBLEM FIRST

HARBOR TECHNOLOGY GROUP

Virtual CISO

What is a vCISO? Why does your business need one?

Cybersecurity has become a critical challenge in all industries, so does the role of the chief information security officer (CISO). A fractional or virtual CISO (vCISO) will not only have depth and breadth of knowledge about the threat landscape, tools, and techniques to protect infrastructure and information, but also a unique perspective on how to analyze and mitigate risk.

vCISO Roles & Responsibilities

Instead of waiting for a data breach or security incident, the vCISO is tasked with anticipating new threats and actively working to prevent them from occurring.

The vCISO must work with other executives across different departments to ensure that security systems are working smoothly to reduce the organization's operational risks in the face of a security attack.

Security Operations – Real-time analysis of immediate threats, and triage when something goes wrong.

Business Enablement – from the boardroom to the executive suite to the various lines of business and departments that keep the organization focused, functioning, and moving forward on a day-to-day basis.

Identity & Access Management – Ensuring that only authorized people have access to restricted data and systems.

Governance & Compliance – Making sure all of the above initiatives run smoothly and get the funding they need — and that corporate leadership understands their importance.

Risk Management – Keeping abreast of developing security threats, and helping the board understand potential security problems that might arise from acquisitions or other big business moves.

Security Program Management – Keeping ahead of security needs by implementing programs or projects that mitigate risks — regular system patches, for instance.

Legal & Human Resources – Determining what went wrong in a breach, dealing with those responsible if they're internal, and planning to avoid repeats of the same crisis.

Security Architecture – Planning, buying, and rolling out security hardware and software, and making sure IT and network infrastructure is designed with best security practices in mind.

More Information:
www.harbortg.com

Contact Phone:
(609) 429-0842

CYBERSECURITY
A BUSINESS PROBLEM FIRST