Defensible

Increase Security and Lower Costs With CISO as a Service

CISO as a Service, also called a virtual chief information security officer [vCISO], offers the same 360-degree cybersecurity coverage as a full-time, onsite CISO at a fraction of the cost.

Benefits of a vCISO

A full-time CISO can cost over $200,000 per year — a price well out of reach for many small or even mid-sized businesses. A vCISO, on the other hand, provides experienced, C-Level leadership on security initiatives on an as-needed basis.

If you can benefit from a CISO, you can benefit from a vCISO. An effective vCISO should provide both tactical and strategic support in managing risk for an organization. A vCISO can provide guidance during a short-term crisis, such as incident response or investigation after an attack, or drive long-term security initiatives like compliance, security education, vendor oversight, or security program creation.

Defensible vCISO Services

A Defensible vCISO can perform the same roles in your company as a staff CISO. These capabilities include:

Security Governance Assessment and Advice

Information Security Risk Management:

Risk management is a core function of an information security department. A Defensible vCISO can help you implement a governance program, determine acceptable levels of risk, review assessments such as audits and penetration tests, develop a risk profile, and prepare you to make impactful security decisions.

Information Security Policies, Standards, and Metrics Review:

Establishing and disseminating information security policies and standards is critical to managing risk. A Defensible vCISO can help assess existing information security and incident response policies compared to relevant industry and regulatory standards.

External Attack Surface and Public Profile Assessment:

Part of determining risk is knowing what attackers see. A Defensible vCISO can lead an effort to identify and document your publicly available risk profile and external attack surface.

Information Security Advice and Response:

Information security issues arise unexpectedly and in a variety of areas. A Defensible vCISO contributes ongoing guidance around threats and risk, recommends practical security solutions as your business grows and changes, and provides rapid guidance and leadership in case of an incident or data breach.

Security Program Roadmap, Implementation, and Operations

Third Party, Cloud, and Vendor Security Review

In the era of cloud, a modern security program requires vendor management. A Defensible vCISO will assess your current approach, review vendor acquisition and integration workflows, and develop processes to align and integrate with the risk management and governance structure.

Detailed Controls Assessment

A security program must track and assess the controls in place. A Defensible vCISO can help you assess how controls are functioning and how well controls are aligned with information security standards. They can drive projects to achieve compliance and effectiveness.

Risk Register, Security Project Definition, and Implementation

Security leadership should help identify, prioritize, and develop projects. A Defensible vCISO works with you to create an itemized and prioritized risk register, identify projects that address those risks, and develop a prioritized roadmap to drive security initiatives.

Monthly Information Security Updates

A successful program requires regular updates. A Defensible vCISO provides structured reports containing security program updates as well as significant and time-sensitive security issues.

Contact Us Today

Defensible Technology helps organizations protect information, trade secrets, intellectual property, and confidential communications from cybersecurity threats. Get started with Defensible today, and see for yourself how a Defensible vCISO can strengthen your security.

Get Started With Defensible
www.defensible.tech