Virtual Chief Information Security Officer (vCISO)

Ensuring the security of confidential data including your customer's sensitive personal and financial details requires constant attention. And though not every business demands the full-time commitment of an executive to oversee this function; small- to mid-sized organizations need the same level of security and intelligence already in place at larger corporations.

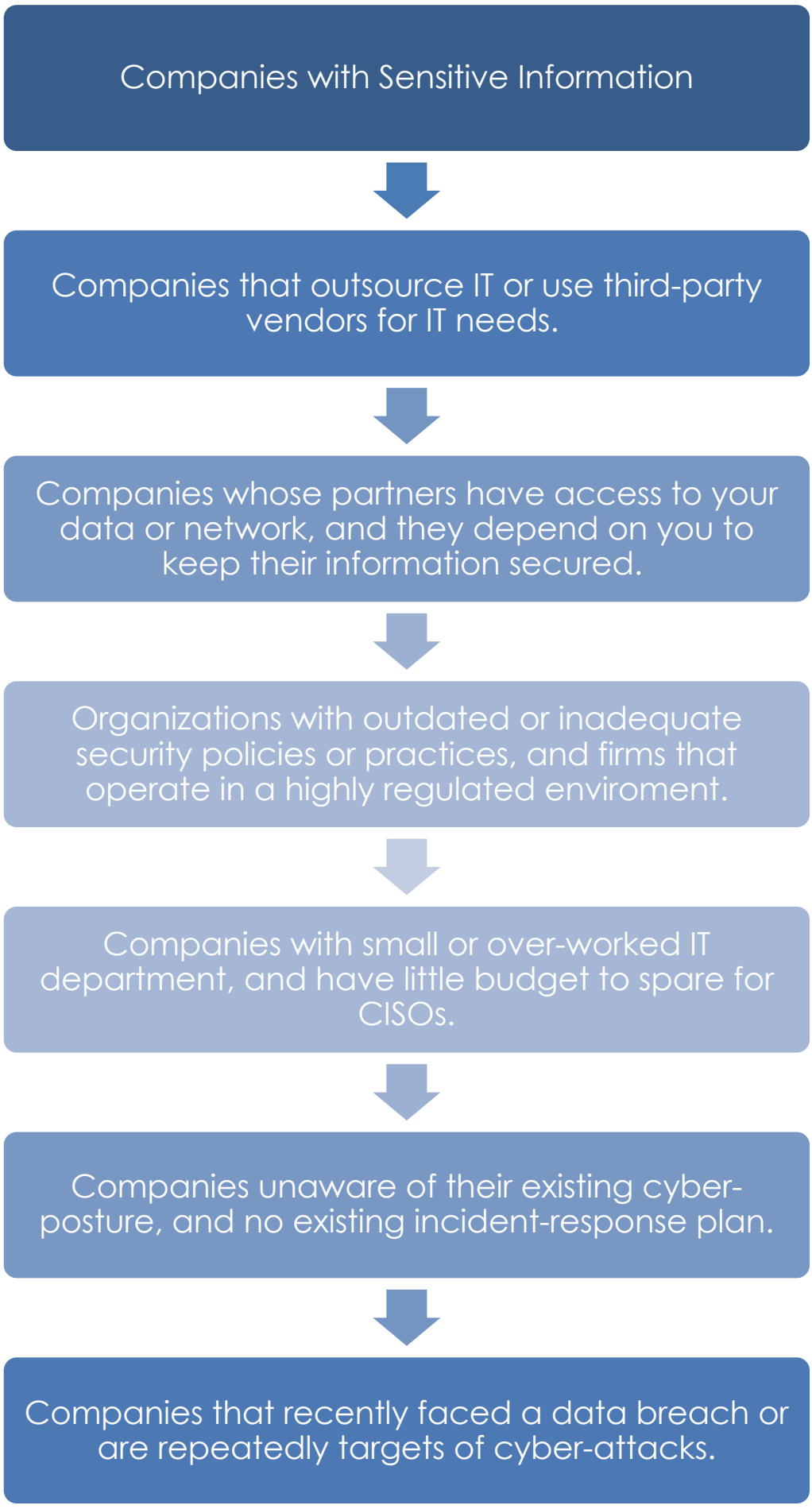
We can protect your organization at the same level you would expect from a full-time chief information security officer through our Virtual CISO service without the steep investment of executive compensation and their associated benefits package. Median salary packages for CISOs are upwards of 500,000 USD, making vCISO services affordable and business friendly for SMEs.

Work in collaboration with an advanced vCISO professional able to maintain a relationship with your team and become familiar with both your environment and industry so you stay on top of constantly evolving threats and regulations.

PLETHORA digital technologies

Unit 458 Kyalami, Maple Avenue,
Midrand, Johannesburg,
Gauteng, South Africa

+27 760 564 128
info@plethoradigital.tech
www.plethoradigital.tech


Companies with Sensitive Information
Companies that outsource IT or use third-party vendors for IT needs.
Companies whose partners have access to your data or network, and they depend on you to keep their information secured.
Organizations with outdated or inadequate security policies or practices, and firms that operate in a highly regulated enviroment.
Companies with small or over-worked IT department, and have little budget to spare for CISOs.
Companies unaware of their existing cyber-posture, and no existing incident-response plan.
Companies that recently faced a data breach or are repeatedly targets of cyber-attacks.

vCISO Components:

Cyber Program Management

- **Build a Strong Program:** Our security program services bring decades of experience in security development directly to your team. Building a security program starts with the definition of security in your organization, and we provide support in establishing this definition and assessing how it appears in your existing security program. Our team stays on top of the rapidly changing security landscape to help your organization develop a customized program that actually works.
- **Assess Your Security Program:** Assess your existing security program against best practice frameworks such as NIST Cyber Security Framework. Recommendations are made based on any gaps or improvements to be made in the security program based on the Cyber Security frameworks and are used to develop a roadmap to achieving your ideal security program state.
- **Understand Your Current State, build a Plan for Success:** A thorough security program assessment is the first step toward developing a more efficient security program. Use a security program assessment as a tool to create a timeline and roadmap to bringing your security program to an ideal state with mind to regulatory and customer requirements as well as organizational initiatives.
- **Develop Your Security Program:** Once you've received your custom roadmap, build or improve your security program with your in-house team. If you don't have your in-house security resources or expertise, this option is right for you. Outsource your implementation to our expert security team. We'll put together the different parts of your security program components.

Optimized Third Party Cybersecurity Management Program

- **Third Party Cybersecurity Assessment:** A vendor risk management program allows your company to manage and monitor all your vendors and interactions. As third-party relationships continue to grow, businesses need to be proactive in developing multi-faceted programs that secure their networks.
- **Secure Remote Access during COVID-19:** One of the key components of a vendor risk management program is secure remote access. Through the implementation of best practices and protocols around secure remote access, companies can ensure that their organization and third-party vendors are secure and compliant while reducing the risk of cyberattacks and costly liabilities.
- **Evaluate & Manage Risk:** Our vendor risk management services are designed to provide a comprehensive evaluation of the security risks that a third-party organization may present. Get the Cyber risk performance assessments you need to efficiently manage your third-party risk. Now Partner, supplier, and vendor security risk is a major area that cannot be ignored as a business issue any longer. Our workflow enables you to easily engage your vendors to realize good risk outcomes.
- **Assess Maturity Level with World-Class Standards:** Detailed assessment of the maturity level of the third party's security program with an emphasis on the organization's ability to defend against and respond to Cybersecurity threats affecting its information assets and mitigate the risk of suffering a security breach. We utilize standard security frameworks such as NIST, CIS ControlsTM, ISO, etc.

NIST Cybersecurity Framework Assessment

The NIST cybersecurity framework (CSF) is designed to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks. As an independent, third-party cybersecurity and compliance firm, PLETHORA can help you navigate the NIST CSF assessment process. With a deep understanding of the NIST cybersecurity framework, our auditors can guide you through a CSF risk assessment or a formal NIST security assessment.

Cybersecurity Advisory Services

- **Hands-On Expertise:** Hands-on advice from experienced security engineers makes the difference between a formal security policy and a security policy that creates a real impact. We bring our expertise to clear the way for you. Shortage of technical and operational experience in cybersecurity is a huge roadblock for decision-making. **Someone has to ask the tough questions: what are the problems, the risks, and what is the worst-case scenario? We can do that for you**.
- **Strategic Advisory for Your Organization:** We can help you mitigate cybersecurity risks without compromising on usability and flexibility of your solutions. The process starts with defining your cybersecurity goals and choosing efficient strategies for achieving them. Our experienced security managers and engineers will provide strategic and tactical advice. Improve effectiveness of your cybersecurity program, fine-tune secure software development lifecycle in your team, cover fundamental risks, and prevent incidents.

Cybersecurity Incident Response Plan

- **Prepare for cyber-attacks with support from our Advisory team.** Ensure that, when the inevitable breach happens, threats are rapidly contained and any impact on your organization is minimized.
- **Incident Response:** As threats become more sophisticated and pervasive, IT Teams need to be confident they can remediate security incidents as swiftly as possible. Our Incident Response and Cyber Resilience services help you proactively build strategies for preventing and responding to threats. In the event of a breach, your IT security & support team can call on our cyber-response advisors for advice on helping identify, contain, and remediate attacks.

Security Culture as a Service (SCaaS): Make Cyber Safety & Wellness a Culture

- **Cyber Security Awareness Programs are customized for Your Industry,** Organization and/or Stakeholder Roles. From our experience investigating cyber incidents, we have seen how virtually every security compromise can ultimately be traced to a human factor. Our findings are supported by a wide range of annual open-source surveys and reports that show employees and related third parties are responsible for 60%-90% of incidents, including those involving paper data sources and lost devices.
- **SCaaS experts focus on the human risks** most relevant to your organization, whether they be industry-related or role-based. You can expect us to have frank discussions with leaders and a cross-section of your staff about digital and physical security factors that put data at risk. In fact, this emphasis on communication is a fundamental part of our approach to building a security culture.