Cyber security systems and principles are designed to safeguard company data, websites and web applications from attackers seeking to disrupt, delay, alter or redirect the flow of data. These attackers vary in target, motive, levels of organization, and technical capabilities, requiring public and private organizations to adopt ever-increasing measures to prevent cyber-attacks.

Over the last five years, the number of cyber-attacks on businesses increased by 144%, the cost of cybercrime per company has increased by 95%, and the average time to resolve incidents has increased by 221%.1 Faced with the reality of this increasing threat, Additionally, a stream of large corporate breaches, including Target, Home Depot, eBay, JP Morgan, Sony, Equifax and others, exposed critical vulnerabilities that ignited investor and C-Suite pressure, demanding firms to act.
THE PROGRAM

As a trusted and premier managed security provider to organizations at every level, we saw the need to not only leverage our expertise in cybersecurity, but also create a program specifically aligned with the SEC OCIE, ISO, and NIST, allowing us to identify and notify you of risk earlier, and your investors could sleep at night. CyberSecOp’s our Cybersecurity Readiness Program is a proactive, methodical approach to cybersecurity, under the direction of a virtual CISO, which aligns the program to the business goals and drives clients toward compliance. Through Risk Assessments, Penetration Testing, Security Architecture, and more, we’ll spend 24 months getting you and your environment fit. You’ll begin seeing immediate results within the first few months, and each month that follows you’ll be put through exercises, seminars, testing, and briefings that will continue to develop fitness at a digestible level.

TRAINING AWARENESS

Employees are part of an organization’s attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. If an organization needs to comply with different government and industry regulations, such as FISMA, PCI, HIPAA or Sarbanes-Oxley, it must provide security awareness training to employees to meet regulatory requirements.

We begin by evaluating your firm’s information security program, policies, workflows, vendor relationships, security architecture, and user awareness. These functional areas are then measured against the NIST Cybersecurity Framework and the 28 areas of interest from the SEC OCIE Risk Alert. Consider the first six months of CyberSecOp’s SEC Cybersecurity Readiness Program as boot camp, where we provide you with deliverables that help you respond to investors and the SEC Risk Alert. The remaining 18 months is training and conditioning, helping your firm develop tier one cybersecurity habits. Activities include:

- Security Risk Assessment
- Penetration Testing
- Policy Review & Development
- Social Engineering Testing
- Incident Response Testing
- Security Awareness Training
- Security Architecture Review
- Audit Assistance
- Vendor Assessment
- Security Operation Center
- Configuration Management, Design, and Remediation
- Monthly Security Strategy Review Calls
One or two internal security engineers don’t stand a chance against the thousands of advanced hackers out there dedicated to breaching your network. You need an army—no ordinary battalion will do. You need rigorously trained, hardcore, unshakeable, obsessed cybersecurity special forces. Meet CyberSecOp Security. Our team has over 20 years of security experience, including deep PCI, HIPAA, ISO, and NIST expertise. We eat security and compliance for breakfast. Additionally, our proactive relationships at the SEC ensure we have a direct line to the latest and greatest intelligence. We’ve got you covered.

Virtual CISO / vCISO
You get the benefit of multiple world-class CISO expertise and highly specialized security talent for a fraction of the cost of a full-time staff member.

CyberSecOp team has extensive experience with security leaders from a variety of industries, and we apply their knowledge to provide you a Virtual CISO services. Working directly with your team, no matter the size, your Virtual Chief Information Security Officer (vCISO), will help strategically plan, and execute the cyber security strategy that aligns with your business strategy. With our guidance, your organization will realize the best strategy to securely enable and support the business, while still dramatically reducing information security risk and inefficiency.

Why CyberSecOP?
CyberSecOp cyber security consulting services was founded by two information security professionals, and a Managed Services IT firm, they recognized the need for cyber security consulting services for small and medium-sized companies, they understand that small and medium businesses need to be secured with an information cyber security program.

CyberSecOp integrity is the baseline upon which our core values are built. Integrity is a fundamental, non-negotiable requirement of employment, and an expectation of suppliers, partners, and customers, both internal and external. An essential aspect of our brand promise is that we always engage with integrity.

Trusted relationships thrive in an environment that demands mutual respect, and we cultivate these relationships among all with whom we do business. We treat each other courteously, act in good faith, and expect others to do the same.

For more information, please contact:

866-973-2677 | sales@CyberSecOp.com | www.CyberSecOp.com