CyberSecOp

Virtual Information Security Officer (VISO) Services

A Tumultuous Year

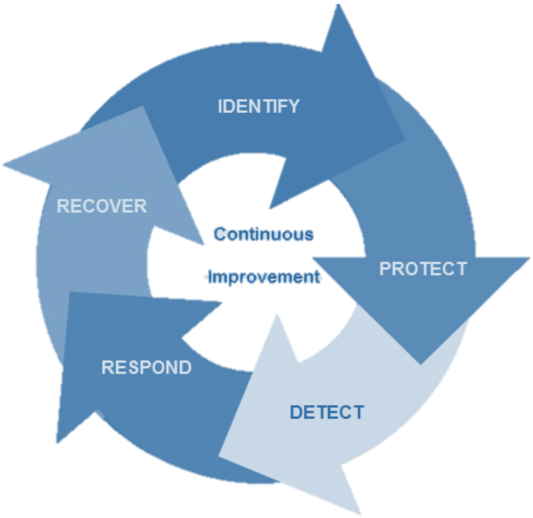
The final days of 2020 have proven even more difficult than anticipated with the COVID19 pandemic, and the recent exposure of the world's latest serious nation-state cyberattack. This latest cyber-assault is effectively an attack on the United States and its government and other critical institutions, including security firms. It illuminates the ways the cybersecurity landscape continues to evolve and become even more dangerous. As much as anything, this attack provides a moment of reckoning. If the American government was breached in such a high-profile manner, what does that mean for your firm?

That's where we come in.

CyberSecOp Virtual Information Security Officer (VISO) Services

As small and large organizations alike, face countless numbers of security threats which may lead to security breaches. To give you an advantage, we would like to ensure your organization is aware of the Information Technology Security Services that CyberSecOp offers: from ISO, ITIL, and NIST-compliant-individual-policies to full security programs, including Virtual Information Security Officer (VISO) services. Thereby ensuring your organization's assets are secure and in compliance by meeting regulatory requirements and protecting your clients' data, effectively providing your firm an edge over your competitors.

CyberSecOp's VISO Security Program, and its Security Control Services, enables your organization to stay ahead of cyber threats, meet regulatory requirements and allow you to focus on your core business.



CyberSecOp's VISO services offer all the following:

- ✓ **Information Security**

  CyberSecOp offers protection for your password information, email usage, and reduces phishing emails.
- ✓ **Risk Management**

  Identification, assessment, and prioritization of risks, as well as Coordination of resources to minimize, monitor, and control the probability of damaging events.
- ✓ **Compliance Assurance**

  Assist organizations in adhering to compliance requirements, with policies accepted by ISO, ITIL, NIST and GDPR.
- ✓ **Data Protection**

  Keep your assets safe with CyberSecOp's email, endpoint, network, and cloud data security services.
- ✓ **Privacy/Classification Programs**

  Categorization of sensitive or restricted data, leading to better business dynamics and employee focus.

Is your organization prepared for the upcoming year?

Data breaches are on the rise, and organizations of all sizes and industries are being attacked daily. CyberSecOp's 10-Step Security Boot Camp can help you get there. We understand and we can assist organizations like yours become secure and prepared to prevent cyber criminals from attacking.

Today's changing security landscape

CyberSecOp's 10-step Cybersecurity Framework is not meant to replace existing processes. It is used to align with existing business processes and ensure that cybersecurity programs address all elements of an organizations as defined in the core framework. Additionally, CyberSecOp's Cybersecurity Framework assists organizations in adhering to compliance requirements. Many regulators have mapped their security controls to the Cybersecurity Framework.

Our security team will provide security governance, audit, risk management, emerging cyber threats, and information assurance management. We have the expertise of over 40 years of combined experience in securing and supporting business technologies.

Our Team of Experts

Our security team provides security governance, auditing, risk management, protection from emerging cyber threats, and information assurance management. Our staff has a combined 40 years of expertise, securing and supporting business technologies.

- Network Certified
- Microsoft Certified
- Ethical Hacking Certified
- Security Certified
- Linux Certified
- ISO Certified

CyberSecOp Services

- **LocViso™**
  Virtual Information Security Officer
- **LocPar™**
  Security Operations Center
- **LocSecure™**
  Incident Response Services
- **LocVM™**
  Vulnerability/Penetration Testing

RISK MANAGEMENT & COMPLIANCE

FEATURES	BENEFITS
Organization & Authority	Define roles and responsibilities
Policy	Establish appropriate policy and oversight
Audit & Compliance	Compliance and security audit leadership and oversight
Risk Management & Intelligence	Proactive identification of new threats, vulnerabilities, and risks
Privacy	Delineation of information privacy compliance requirements
Incident Management	Communication, response and resolution of information security events using an Incident Response Plan (IRP)
Operational & Technical Security & Access Control	Deployment of technical and access controls
Physical & Environmental Security	Protection of physical assets
Asset Identification & Classification	Creation and planning and operational procedures related to inventory, accountability, responsibility, classification, and implementation of associated controls
Account Management & Outsourcing	Creation and implementation of policy and procedures governing the hiring, transfer, separation, and clearance processes for employees, contractors, and vendors
Monitoring, Measurement & Reporting	Definition and documentation of the controls that define the event information that will be logged and reported
Education & Awareness	Delivers the planning, procedures, documentation, and implementation of security awareness and related training for employees
Mobile Device Management	Mobile device support and reporting. Auditing mobile devices and applications to track compliance with enterprise policies. Tracking usage of services and apps. Mobile access provisioning/removal, remote wipe, and data flow control to revoke user access to mobile applications and information in the event the user or device becomes untrusted
Security Information and Event Management (SIEM)	Event Logging & Correlation, Intrusion Detection, Unauthorized Access Detection, Event Investigation
Vulnerability Management	Internal & External Vulnerability Assessment, Windows Patch Management, 3rd Party Application Patch Management, Patch Reporting (Successful/Missing/Failed Patches)
Managed Service Desk	Unlimited Remote Service Desk Support, Trending and Reporting Information, Capacity/Status Reporting
Data Classification	Implement a comprehensive Data Classification scheme to assist in securing and managing information according to its sensitivity and value to your organization.
Data Loss Prevention (DLP)	Audit logging of data movement, Data classification, Data movement restriction, Data compliance governance

Contact us

Headquarters:
5 Hillandale Avenue
Stamford, CT 06902
CyberSecOp.com
Sales@CyberSecOp.com
866-973-2677