CAPRICORN CYBER SECURITY SOLUTIONS

CIP| Information Assurance (IA&A) |Vulnerability Assessments| CISO On-Demand

Critical Infrastructure Protection (CIP)

Capricorn Systems, Inc., has over two decades of expertise at developing and implementing Critical Infrastructure Protection solutions. We adopt a holistic, system-of-systems approach to ensuring the reliability, security, and resilience of critical infrastructures. Our teams have helped large Public Sector clients (who own most critical infrastructures) to anticipate, defend against, and recover quickly from attacks on their physical and cyber infrastructures while maximizing profitability.

Information Assurance (IA&A)

On the IA&A area, success as a provider of Cyber Security/Information Assurance results from industry leading security solutions, procedures and expertise. Our team develops and delivers custom security solutions that assist organizations in prevention, detection and mitigation of effects from a cyber-attack. IA&A & Additional Cyber Solutions at Capricorn include:

- Custom Security Assessments
- Network Modeling
- Security Policy Development/Management
- Custom Integration of Technologies
- Intruder Detection

Vulnerability Assessment & Penetration Testing (VAPT)

Capricorn’s 'Vulnerability Assessment and Penetration Testing' service uses a combination of state-of-art tools like Accunetix WVS, Metasploit Pro, Nessus Professional, Backtrack etc, and experienced ethical hackers with appropriate certifications like CEH. It helps enterprises conduct intelligent 'Vulnerability Assessments' and 'Penetration Tests'.

Our ethical hackers have many years of experience in this field and have exposure to a wide range of industry verticals and operating systems, applications, networks and security devices. They are selected after stringent background checks and their expertise is used to help our customers identify and take action on vulnerabilities and weaknesses in their IT assets and Information Security Management System (ISMS). They can conduct black box, gray box and white hat penetration tests to help customers improve their security infrastructure and information security policies

CISO On-Demand / Virtual CISO Services

Capricorn provides its CISO on Demand services on an as-needed basis, be that to cover for an interim CISO appointment or to accomplish specific tasks, including:

- Interim CISO Services
- Creating/ updating IT Security policies
- Managing IT risk against business goals
- Cybersecurity training
- Reducing overall risk posture
- Securing sensitive data
- Developing a robust security program

CYBER SECURITY & INFORMATION ASSURANCE OFFERINGS

Service Type	Service Description
Business Continuity Planning	Deliver expert level BCP efforts in order to provide a repeatable, customized, and executable business continuity plan
Disaster Recovery Planning	Outsourced or co-sourced DR planning against logical and physical threats to business continuity.
Business Impact Analysis	Work with Finance, Operations, and Risk Management in order to derive business impact levels that result possible security compromises.
Redundant Data Storage	Provide redundant cold or warm site to client with <500TB of data needs
Virtualization Services	Virtualized Data Solutions (priced per user)
Business Process Engineering	Engagement aimed to streamline security and compliance efforts without jeopardizing the integrity of the ISM program, compliance levels, or security posture. Intent is to increase efficiency in security management.
S-SDLC/SDL-IT	Work to develop a secure SLDC or Secure Development Lifecycle for client's development teams. Training hours encompassed to address key application threats & vulnerabilities that should be repeatedly addressed by SLDC/SDL-IT Process.
Compliance Audits	Provide audits against regulatory requirements for security (does not include SOX, PCI - Sold separately).
SOX Testing	Pre-audit SOX testing of enterprise level controls
PCI Readiness Assessment	Pre-audit PCI Testing of controls mandated by PCI-DSS
Data Privacy Assessments	Assess impact of process/control related security vulnerabilities in order to derive data privacy impacts
Governance Related	Development of security policies, standards, guidelines and other enterprise wide or issue specific artifacts that sustain security governance and the ISM program (does not include secure coding standards)
Maturity Modeling	Measure maturity levels of processes and controls relative to maturity models.
Benchmark Testing	Measure existing security/ compliance controls against an internal defined or externally defined benchmark or framework of controls.
Security Awareness/ Training	Outsourced security awareness training or development of security awareness materials that are tailored to client environment and business
Security Architecture Services	Provide security architecture expertise on client server application environments within private, semi-public, and public networks.
Secure Coding Standards	Develop a tailored secure coding standard encompass key programming languages for client.
ISM Program Dev	Develop a sustainable and tailored ISM program for clients
Intrusion Handling & Response	Provide intrusion detection and analysis of client networks and encompassing assets in order to derive source, problem, and remediation planning efforts.
Forensic Analysis	In-depth forensic analysis of data retrieved from client networks in order to clearly identify issues related to cause, accountability, and likely attack patterns used. Customizable for legal response
Risk Assessment Services	Application of risk assessment methodology to derive business risk resulting from security threats or incidents.
Vendor Risk Assessments	Security risk analysis against client vendors in order to identify high risk vendors, assign risk priorities, identify risk issues, and broker remediation efforts.
Threat Modeling	Apply PASTA risk centric threat modeling methodology and correlate to software and security workflows based upon risk levels derived threat analysis and likely attack patterns identified for a client application environment or set of environments. Integratable with SAMM maturity modeling.
Hybrid Risk Assessment	Advanced risk assessment that is aimed to correlate risk analysis efforts across multiple technology and business domains in order to identify and quantify financial risk levels to client risk managers.
Remediation Management	Outsourced service for managing remediation workflow and providing assistance with HIGH risk remediation items via client change control procedures
M&A Security Assessment	Assess security posture of company to be acquired or merged with client organization.
Vulnerability Assessments	Provide vulnerability scanning services to clients wishing to identify network and platform related security weaknesses or holes.
Penetration Testing	Application of exploitation frameworks in order to exercise attacks against discovered network and platform related vulnerabilities
Web Application Testing	Manual Testing, Business Logic Exploitation, Fuzzing Techniques to identify weaknesses in web applications and the underlying DOM calls made to other layers of the application environment. Expose programmatic and architectural application flaws for web applications.
Source Code Analysis	Manual review of code sets in order to derive possible security holes in programming logic and function.
Red Teaming/ Social Engineering	Provide social engineering attacks in order to identify holes in security awareness amongst company personnel. Conducted in person, over phone, email, IM, and SMS

Please email info@capricornsys.com or call us at 678-689-0936 for additional information on our Security Offerings or to schedule a call with one of our Cyber Security Experts.