Supply Chain Cyber Risk Management Services

The risks to the U.S. Government are increasing as a direct result of doing business with the supply chain (Government Contractors), especially small businesses. These contractors are sustaining more damaging breaches by hackers and nation state actors because of their access to sensitive, proprietary, or classified data. Many Contractors struggle with the costs associated with having enhanced cyber risk mitigation strategies. HEMISPHERE can assist you offset these costs.

In an effort to meet the needs of the Government, HEMISPHERE Cyber Risk Management Corporation LLC (HEMISPHERE) has designed a packaged solution tailored for contractors that support the United States Government as a supply chain partner.

In December of 2015, the Department of Defense instituted an update to the Defense Federal Acquisition Regulation (DFAR) requiring defense contractors that sell to the Defense Department to demonstrate adherence to the NIST Special Publication 800-171 "*Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations*". Since December, both the Federal Acquisition Regulations (FAR) and the National Archives and Records Administration (NARA) have amended their definition of CUI. Our assessment methodology provides an option for supply chain partners to rapidly meet the Government's desired outcomes of enhancing their security posture and lowering the Government's risk surface. These requirements have since evolved into requirements now defined by NARA.

The outcomes from our assessment demonstrates how your organization successfully meets these goals and outcome of 800-171 and our findings provide a cost benefit analysis allowing for prudent investment strategies in addressing cyber risk management.

Regardless if you want to identify vulnerabilities or demonstrate exploitation through tools, tactics, and procedures used by hackers, simply running a tool-generated report will likely not convince senior leadership that immediate action is needed. This is where we excel.

We accomplish this by transforming cyber security into more of a "*risk management*" approach. This approach also allows you to demonstrate conformity to NIST SP800-171 as well as have enhanced levels of assurance meeting data breach requirements as defined by 48 states. Every business evaluates how much it spends in relationship to how much it earns. Cyber is no different. Using our model allows business owners to understand the costs associated with remediation versus incident response enabling business and cost justified decisions on security program investment strategies.

Our clients rate us with superior past performances in terms of quality and cost when compared against competitors and internal levels of effort.

HEMISPHERE

Your Gateway To Cyber Risk Management

www.hemispherecyber.com

Supply Chain Cyber Risk Solutions

⇒ **Easy to implement**

⇒ **Actionable**

⇒ **Lowers your operations cost**

⇒ **Lowers your risk surface**

HEMISPHERE's robust framework positions our clients for success. We accomplish this by applying lessons learned from other's mistakes. This enables reductions in your total cost of ownership and enhancing operational fidelity.

Making Cyber Risk Operationally Relevant

Implementing Cyber Risk Management as a "Cost-Avoidance" Mechanism

Your Gateway To Cyber Risk Management

www.hemispherecyber.com

Supply Chain Cyber Risk Assessments for Government Contractors

To meet the needs of the United States Government, we have designed an approach that provides the supply chain with a more mature capability in assessing risk than traditional assessments (including penetration testing).

Service	Traditional Assessment	HEMISPHERE
Pre–Site Analysis	X	X
Onsite Technical Assessment to identify gaps when measured against NIST SP: 800-171	X	X
System Security Profile (SSP) Generated	X	X
Vulnerability Scan (Nessus)	X	X
Business Risk Analysis of scan results		X
Certificate of Assessment		X
25 additional controls evaluated that have the highest likelihood of resulting in a cyber event when not followed		X
Legal/Litigation Exposure Analysis		X
3rd Party Business Partner Risk—SLA and T&C gap analysis*		X
Cost-Benefit Analysis		X
Robust Security Assessment Report (SAR) that can be used to reduce cybersecurity insurance premiums with attorney-client protections		X
Formal Debrief to Ensure Knowledge Transfer with C-Suite		X

*** SLA—Service Level Agreements T&C—Terms and Conditions**

Today's business environments can no longer afford to focus on trying to defend against highly organized, well-funded, and highly skilled adversaries by simply using antivirus and perimeter defense techniques. Providing higher assurances of operational fidelity can only be achieved through a strategy ensuring you have the capability to identify, protect, detect , respond and recover. Because these capabilities are generally cost intensive, business owners apply "reactive" approaches versus "proactive".

HEMISPHERE's capabilities allow us to translate cyber threats into business risk demonstrating total cost of ownership reductions for your security and risk investment strategies. Contact us today for a free consultation. Email: contact@hemispherecyber.com Office: (703) 881-7785

10432 Balls Ford Road, Suite 300

Manassas, VA 20109

United States