MAUREEN DATA SYSTEMS

EXCELLENCE THROUGH TECHNOLOGY

RANSOMWARE & SUPPLY CHAIN INCIDENT MANAGEMENT

MDS is a woman-owned and WBNEC-certified technology driven and solution-based company. We provide our clients **state-of-the-art information security**, management, and privacy solutions to **combat cyber threats and promote business resilience**. We take an **offensive and defensive** approach to information security, governance, risk, and compliance. This approach is critical to combat ransomware and supply chain incident management.

WHY DO YOU NEED AN IR PROGRAM?

Our comprehensive Incident Response (IR) and Cyber Program is the **preemptive strike against nefarious actors**. By identifying your organization's vulnerabilities and conducting a business impact assessment, MDS can remediate the vulnerabilities and a tailor the IR policies and procedures to address your organization's needs. A written IR Program serves as evidence of good faith efforts, and such documentation will be a **will be a condition** to secure cyber liability insurance. Moreover, such documentation may be **necessary by law** and/or **may mitigate sanctions and/or penalties**, should a regulator or enforcement agency allege noncompliance or negligence.

WHY MDS?

Our agile approach to developing an IR Program is from an external adversarial perspective. Understanding an organization's vulnerabilities is just the start of proactive incident management. Our solutions and **cost-effective** tools streamline your organization's IR, Business Continuity Plan (BCP) and compliance requirements.

OUR SERVICES

- **BLOCK 64.** Utilizing Microsoft's Block 64 technology, MDS can obtain an inventory of your current information assets and infrastructure, including desktops, servers, vCenters and network infrastructure. By leveraging Microsoft's technology, MDS can discover and remediate any non-compliant patch levels, unprotected endpoints, and/or currently exploitable vulnerabilities. Coupled with our C3RES solution, MDS provides your organization an unparalleled and comprehensive solution to enhance your cyber resilience and any third-party vendors within your supply chain.
- **C3RES.** Using our Continuous Comprehensive Cybersecurity Risk Evaluation Services (C3RES), we assess the organization's supply chain. A C3RES assessment will provide leverage over third-party relationships, which will influence negotiations.
- **RSI.** The Ransomware Susceptibility Index (RSI) determines how likely your external facing infrastructure is seen by an adversary and the likelihood that to be compromised by Ransomware. Through the RSI, we will gain recon and competitive intel to protect your organization from financial and reputational damage, including threats to national security.
- **REMEDIATION.** Depending on the findings from Block 64 reports, including the C3RES & RSI assessments, remediation services are available upon request.
- **BUSINESS IMPACT ANALYSIS (BIA).** Review existing incident policies and procedures. Define all services, applications, assets, network technologies, and rank level of importance. Establish formal IR Management Program and BCP. Establish roles and responsibilities.
- **DEVELOP.** We will develop your organization's policies and procedures as it pertains to incident response.
- **PROTOCOLS.** We will facilitate a variety of pre-planned responses that will help your organization understand the maturity pathway and importance of IR. Incident Management will facilitate what weaknesses were found and need to be addressed to bolster this process.

- Assess your team's readiness for an incident
- Define the process for updating management according to your organizational requirements for all stakeholders including CEO, IT, Legal, HR, Finance, Compliance Marketing, PR, Supply Chain, etc.
- Identify and correct planning and procedural deficiencies
- Build strengths by checking the activity and logging of Indicator of Compromise (IOC)
- Ongoing management of an incident including monitoring of time frames
- Improve coordination and communicative efforts between internal teams
- Monitor the activity and IOC timeline logs, complete with chain of custody of IOC and artifacts stored in a single, secure repository
- Tailor generated reports to suit your legal and compliance requirements
- Integrate lessons learned from previous incident management

contactus@mdsny.com (646) 744-1000 www.mdsny.com