SENEDIA TECH TALKS:

Panel Discussion on DFARS and NIST Security Requirements and Compliance

Tuesday, 11 April 2017

SENEDIA hosted a series of presentations, followed by a panel discussion on the technical, contractual and business requirements of the DFARS and NIST regarding the safeguarding covered defense information and cyber incident reporting. On 21 October 2016, DoD published the latest requirements to prevent improper access of important unclassified information in the supply base, to be implemented by 31 Dec 2017.

Presenters and panel participants included:

- Stephen Ucci, Counsel, Adler, Pollack and Sheehan P.C. and member of the Rhode Island House of Representatives;
- Christopher Michaud, Engineering/IT Department Head, McLaughlin Research Corporation (MRC)
- Richard Astle, Mechanical Engineering, McLaughlin Research Corporation (MRC)
- Mike Carmack, Cyber Security Analyst, RITE Solutions

The first speaker was Stephen Ucci, who discussed cybersecurity issues and threat mitigation advice for any company who deals with controlled unclassified information (CUI). Stephen is the Chair of the Government Contracts Group for Adler, Pollack and Sheehan, and centered his presentation around the NIST 800-171 Compliance, and DFAR 252.204.7012. Stephen highlighted various examples of serious cyber issues, threat actors, and the important of cyber security considerations when getting a product to market. As threats are evolving and associated risks are increasing to all companies who generate and utilize sensitive data, it is imperative that companies stay abreast of not only the latest technologies and developments, but also the ever-changing threat environment. As discussed, cyber security impacts, and is an important consideration, for every part of a company, and the issues and implications are not contained to IT departments. The vulnerability today is shared by Government, Industry or a private person, alike.

Stephen discussed the importance that this challenge be acknowledged from the top of any organization, essential to building a culture of vigilance by all, and an approach to cyber security that emphasizes continuous improvement and knowledge sharing. Too often it is the human element that allows for the vulnerabilities we face in the cyber world. From social engineering of bad actors, to carelessness, misplaced trust and lack of training, people are at the heart of both threats and cyber safety. The basics of sensible policies, training and awareness, gaming and testing, and security incidence response planning, are key to cyber safety.

Specifically, 15 requirements from NIST SP 800-171 are applicable to all acquisitions other than COTS. The DFAE 252.204-7012 requires full compliance with NIST 800-171. In the case of a data breach, a company has 72 hours to report cyber incidents to the DoD CIO, preserving evidence and offering full disclosure and cooperation with the agency. The company must also make all suppliers and partners aware, for their own data protection. Unclassified data that must be protected is defined by DFAR 252.204-7012, and includes a fairly broad definition of the data that falls into this category, including

"any other information marked or otherwise identified in the contract that requires safeguarding or dissemination controls." "Families" of security requirements include access control, physical protection, incidence response, personnel security, risk mitigation, media protection, identification and authentication, audit and accountability, awareness and training, and more.

Rhode Island is in the forefront of cyber security, with thoughtful and impactful legislation on data protection. Stephen discussed how Congress has permitted companies to perform forensics to allow them to figure out who has done hacking, when there is a security breach. He discussed the importance of the US Cybersecurity Information Sharing Act which is a federal law to improve cybersecurity in the US through enhanced sharing of information about cybersecurity threats, and for other purposes. This law allows the sharing of internet traffic information between the US government and technology and manufacturing companies.

The second speaker was Chris Michaud who discussed the importance of taking an engineering approach to cyber security and data protection, looking systematically at requirements and actions that impact everyone in a company, and all partners in a supply chain. From a problem-solving perspective, MRC as broken down all the NIST rules to develop their strategy and plan for addressing cyber protection and mitigating risk. Engineering processes helped them to look at the cyber security requirements at the top level, and then dissect each requirement to a series of actionable requirements that they could respond to with solutions. MRC ended up building a tool to facilitate the development of their facility security plan.

Chris highlighted important lessons-learned from their approach:

- The team addressing cybersecurity requirements and protection approaches must look at cyber security threats and requirements from all levels and across all parts of the organization.
- The solutions and implementation team(s) must be diverse, covering practices and business perspectives from all parts of the company.
- It is important to reach out to peers, sharing challenges and best practice solutions.
- It is essential that a company never underestimate what an auditor might inspect or examine; all aspects of a company's cybersecurity plan must be in place, robust, and in practice.

The third speaker was Richard Astle who discussed the complex and sometimes overwhelming world of NIST requirements. He talked about the burden for small companies who do not understand, or are not familiar with the NIST requirements and/or how to address them. There are fourteen categories of high level requirements, that involve approximately 300 controls for data security and protection. NIST 171 maps to 53 requirements. Auditors look at the protection of this data and the accountability of a company to practice and enforce this protection. Often times, small businesses collect data but to not take the steps to organize it and store it in a way that an auditor can perform a sensible audit. Policy and procedures are key, but most important is the regular company practices that demonstrate accountability to the requirements and the procedures a company has in place.

Richard shared that often manufacturing is the weakest link in the security chain. The intention of the NIST requirements is to protect data, at every point along the supply chain. Everyone in the system needs to protect data and to do this, they need to work together. In understanding the NIST requirements and implementing their own system, MRC can now help other companies to develop and implement a system to assist them in complying with NIST requirements.

The fourth speaker was Mike Carmack who handles all IT solutions for RITE Solutions. He tackled their approach to the NIST requirements that must be in place by December 2017. RITE Solutions used CMMI Level 3 processes and approaches to the challenge of data protection and cybersecurity, and utilized the synergy between the two sets of requirements. They had regular meetings and planning sessions, tracking progress and implementation methodically along the way. Tying the approach to ISO 2015 modifications and treating classified and unclassified the same way will help insure that proper measure have been taken to protect data. He spoke of important factors for success:

- There must be buy-in for the cybersecurity priority and approach from the very top of the organization. Senior managers must be engaged and committed.
- There must be a methodical approach that begins with the discovery phase, understanding what controls are currently in place, what controlled unclassified data (CUI) that have and deal with, and where it is in the system. This includes how it is obtained/generated, how it is stored and protected, and how it is retrieved. The entire environment must be examined and assessed for impact on cybersecurity and data protection.
- The company must understand the role of CUI, and the risk associated with various types of data. It is quite possible that the cost of risk mitigation or robust data protection outweighs the cost of the risk itself. A company must make decisions about how much effort and resources to commit to NIST requirements, and do what makes sense to them in their business. A company should consider critical infrastructure, number and roles of employees, the company systems that are in place and critical to their operation, and requirements mapping.
- Through a company's approach and actions, they should demonstrate a robust due diligence that had led to their implementation. A robust process for determining how the NIST requirements are addressed is important.
- Companies should acquire a PKI token to send a breach notification report.
- Companies should pay attention to cloud computing security guidelines and how they relate to NIST requirements and compliant practices. There should be a keen awareness of how the cloud is being utilized within a company. The cloud has evolved, and with current protections, it sometimes is more secure than internal company systems for data storage and protection; however, a company must understand how they are using the clouds and how their data is protected.
- There are over 100 requirements involving information sharing and reach out; the entire supply chain needs to be secure.

Being compliant with NIST 171 is evolving; it is not a static set of requirements. As threats evolve, so are the necessary steps to protect data. Today, unless a problem surfaces, regular auditing from external sources is not taking place. When a problem arises and there is a breach of data security, the audit will look at all data protection practices in a company, which is when ineffective or deficient systems will become an issue. Compliance is critically important for a company to acquire cybersecurity insurance. It makes it more important for a company to perform internal checks to ensure their data is protected and there is adherence to their protection policies and processes.

Cleared companies should perform self-assessment to ensure compliance with the NIST and their own procedures. This is one way a company can demonstrate accountability to data protection. DSS will not

dig into a company's systems, but with any data breach they will have to disclose information on data protection and company practices.

The biggest challenge is remaining efficient in the day-to-day work, while adopting new data controls and cybersecurity processes. Taking a risk-based approach to each new requirement will help a company appropriately scale-up to address the risks identified.

Requirements should be flowed to all subcontractors. Often a company has little control on the practices of a subcontractor, but the guidance is that if there is a reason to know of a security issue or you suspect a weakness in the system, then they must act to protect data. Typically, each part of the chain is asked to certify their compliance.

It is important to have documentation of all practices and systems. The processes in place should be understood, practices, and repeatable.

MRC's tools are designed to help small companies who cannot digest and act on all requirements. The final briefing was an overview of MRC's Cyber Security Appliance, a hardware device provisioned behind a company's firewall designed to supplement a business's network security and auditing infrastructure. The device provides a real-time and proactive approach to network threat monitoring and protection, and advanced threat data analysis and logging, based on the most recent DoD standards and regulations. The interface is a dashboard-style layout with drill-down capabilities allowing in-depth data analysis. Its "Honey Pot" feature serves as a decoy to lure potential attackers away from a company's internal network, and a real-time playback of actions taken by attackers in the honeypot environment. A company can detect, analyze and record detailed data from attempted unauthorized network access, while protecting their company's data.