GUEST COLUMN

The Guest Column features articles written by professionals in the services community. If you would like to contribute an original article for the column, please contact our editor, Jon Williams at jwilliams@pilieromazza.com.

SUPPLY CHAIN CYBERSECURITY RISK IN GOVERNMENT CONTRACTING

By Jason Clark, ISMS Solutions

The digital superhighway is young, relatively unregulated and functions like the Wild West where both public and private sector organizations are experiencing avoidable breaches in their data due to the fact that their information security management systems are incomplete or absent. Implementing adequate cybersecurity controls is an immediate necessity as the cost and effort in developing, implementing and monitoring solid information security practices could be dwarfed by the cost of remediating a major security breach.

It is not just your organization's infrastructure that needs oversite as some of the largest data breaches were perpetrated by hackers gaining entry via third party vendors. Understanding your supply chain's cybersecurity has become critical in defense contracting because on October 30, 2015, the Department of Defense (DoD) issued a Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) which allows the DoD to mitigate supply chain risk by: 1) excluding sources of supply from covered procurements for failing to meet qualification standards or for failing to satisfy evaluation factors; or 2) withholding approval for prime contractors to use certain subcontractors.

While still largely unregulated, the U.S. government, in an effort to protect against attacks, is using its powers to enforce compliance with measures that are constantly evolving. This creates a nightmare scenario as inadequate cybersecurity management systems can have numerous adverse consequences for federal government prime and subcontractors involved in the development or delivery of information technology products and services related to National Security Systems including:

- Cessation of current contracts and inability to win new business
- Loss of proprietary information and data
- Damage to reputation
- Resources needed to remediate the problems

Soon, even more government agencies will require all of your corporate partners, suppliers and data providers to meet specific security levels in order to maintain or retain business for fear of data breaches. Therefore, cyber hygiene across your supply chain is the only antidote to an already infected business population.

Going forward you need to ask your supply chain partners questions such as:

- Does your organization have a process in place for handling and mitigating issues with your information security program?
- Does your organization have a set of information security policies to cover acceptable use, access control, supplier management and incident management policies?
- In the last 12 months has your organization conducted a comprehensive internal audit to look at the effectiveness of your security controls and has top management reviewed the results?
- Does your organization have a policy of encrypting transfers of critical data?
- In the last 12 months has your organization completed a vulnerability scan on network(s) and computing systems?
- Has your organization clearly identified regulatory, statutory, and contractual information security and privacy requirements?
- What type of data does the supply chain partner handle on your behalf and what type of access do they have to your infrastructure?

Continued on page 2

LEGAL ADVISOR

Published by

PILIERO MAZZA PLLC
ATTORNEYS AT LAW

Continued from page 1

Knowing the answers to these and other questions will help determine the risk each supply chain partner poses to your government contracts. Once you understand this risk, the next step is to determine the level of compliance you will require from your supply chain partners. For example, will you require that your supply chain partners to have ISO 27001, NIST, HIPPA, some other security certification or that they match your company security standards? Lastly, you will need to track and verify their compliance on an ongoing basis.

All of this probably sounds quite daunting in terms of procedural know-how and level of effort, but there are products and services, such as ISMS' Conformance Works, which allow organizations a central, online location to manage their own vendor network and to aggregate, authenticate and enhance the level of compliance of their supply chain partners.

Being secure should be every organizations goal. However, in this day and age your corporate partners must also be secure in order to avoid potential disaster so knowing their level of cybersecurity is as important as knowing your own.

About the Author: Jason Clark is the President and Founder of ISMS Solutions (www.ismssolutions.com), a management consulting firm that employs a holistic, organized approach to addressing governance, risk management, and compliance (GRC) strategy and implementation. Specializing in information security, ISMS collaborates with clients to customize, implement and automate information security standards and processes that meet or exceed certification standards. ISMS also has a proprietary information security platform, Conformance Works, which allows clients to manage customized risk and compliance initiatives across their organizations, as well as vendors and other associated companies. He can be reached at jclark@ismssolutions.com.

The *Legal Advisor* is a periodic newsletter designed to inform clients and other interested persons about recent developments and issues relevant to federal contractors and commercial businesses. Nothing in the *Legal Advisor* constitutes legal advice, which can only be obtained as a result of personal consultation with an attorney. The information published here is believed to be accurate at the time of publication but is subject to change and does not purport to be a complete statement of all relevant issues.