Gray Analytics

SUCCESS STORIES

Uncovering Critical Risks While Working Toward Compliance

The Situation

A manufacturing company focused on custom high-powered laser solutions for a variety of applications, including defense, industrial, and scientific markets, needed our help assessing its operations and corporate IT services against industry best practices as well as current and upcoming Department of Defense (DoD) compliance requirements, including DFARS 7012 and Cybersecurity Maturity Model Certification (CMMC). Our client wanted to better understand how it currently measures up to the compliance standards and where it should focus attention and resources to mitigate any potential vulnerabilities.

The Challenge

Our team diagnosed internal risks associated with a limited amount of formalized cybersecurity policies and procedures as well as a reliance on what was only a partial implementation of improper and reactionary security controls, all of which fostered a dangerous false sense of security at the client. Specifically, we discovered:

- Insufficient work from a former outside consultant that left our client reliant on cybersecurity policies and procedures that were limited in scope and outdated, which made effective governance almost non-existent;
- Inexperienced staff tasked with applying largely ad-hoc security controls, which led to a counterproductive false sense of security and minimal actual protection from an attack; and
- Lack of recorded systems architecture and IT inventories, which limited our team's ability to assess risks associated with and the potential impact of failed control systems.

Key Successes

Because of our team's support, our client gained a greater understanding of where it needed to formalize policies and procedures to start building a more secure, efficient, and compliant operating environment. In addition, we helped our client identify where to focus time and resources to ensure compliance with current DFARS 7012 requirements and start preparing for needing to comply with future CMMC-related requirements and obligations.

Our Solution

We relied on extensive personnel interviews and systems reviews to piece together a complete picture of the client's corporate IT and cybersecurity environment since documentation was limited. From there we were able to identify key vulnerabilities and gaps to our client's compliance requirements.

The Outcome

We developed a more complete picture of our client's operational IT environment and used that to perform a controls gap analysis that highlighted key vulnerabilities and areas of concern. We were able to help our client gain a greater understanding for where time and resources should be focused now and in the future to productively and efficiently start working toward compliance with DFARS 7012 requirements and begin preparing for eventual CMMC-related requirements. In addition, we helped our client build tailored communication processes and procedures to alleviate current headaches and vulnerabilities arising from what were historically decentralized and uncoordinated security controls.

GrayAnalytics.com | 256.384.GRAY | info@grayanalytics.com