Gray Analytics

SUCCESS STORIES

Updating Technology & Policies to Keep Up With Modern Threats

The Situation

A manufacturing company focused on deep-hole drilling, boring, and milling services for a diverse set of commercial and government markets asked our team to assess 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 NIST 800-53. We were asked to help the client understand how it currently measures up to the compliance standards and where it should focus time and resources to mitigate any potential vulnerabilities.

The Challenge

We discovered an operating environment in need of organization and a few updates. Cybersecurity policies and procedures as well as several operational technology (OT) systems were outdated and in need of refresh to align with today's technology and best practices. In addition, our client's security control environment, as well as its physical environment, was split across locations and resources and in need of better organization and collaboration. Specifically, we discovered:

- Reliance on an already full-time-staffed employee to provide system-wide, ad-hoc IT support, which limited our client's ability to proactively identify and neutralize threats;
- Outdated cybersecurity policies and procedures that were limited in scope;
- 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;
- Outdated OT systems that had been updated intermittently with bolt-on GUIs and digital control interfaces in the 1990s and 2000s; and
- A multi-site organization structure, which further stressed our client's ability to sufficiently secure and protect its operating environment given its reliance on outdated policies and procedures and limited IT resources.

Key Successes

Our team helped our client organize and update its operations and formalize a more modern set of cybersecurity policies and procedures to form a strong foundation of a secure and compliant operating environment. Our assessment identified a need to update technology and practices to shore up vulnerabilities and allow for more proactive security controls.

Our Solution

To overcome the challenges associated with incomplete systems documentation, we developed a complete picture of our client's corporate IT/OT environment. From there, we completed a thorough gap analysis against our client's compliance requirements. In addition, we provided cybersecurity training to our client's employees to encourage best practices and continued security of operations.

The Outcome

We developed for our client a complete policy portfolio to aid in its adherence to ongoing compliance requirements. In addition, our team undertook a complete systems architectural review and provided recommendations for a more organized, efficient, and secure operation. Further, we advised our client on engineering and physical security improvements that would better utilize resources and ensure continued security and compliance.

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