fortium partners

Case Study

From Fragmentation to Integration: Fractional CIO Enhances Cybersecurity & Operational Efficiency

Client Profile

- International Industrial Products Company
- Founded: 2014
- Headquarters: Dallas, Texas
- Annual Revenue: ~$790M
- Employees: ~2600
- Growth through acquisitions

The Challenges

A leading provider of industrial products faced significant challenges in its operations, stemming from its presence in four countries and reliance on various technology providers.

This lack of service optimization led to fragmented and inconsistent service delivery and cyber risk management across locations worldwide. Each business unit had a different risk mitigation strategy that complicated the development of a cohesive risk management strategy and resulted in unique security practices for different sites.

Additionally, despite the corporate objective to function as a single entity, the businesses continued to operate independently, resulting in operational silos that prevented streamlining services and workflows for operational efficiencies. The diverse and variable technology environments further hindered efforts to implement standardized processes and security measures. Compounding these issues was the absence of a dedicated Chief Information Security Officer (CISO). The dual role of the CIO included cybersecurity responsibilities to discover and address gaps preventing an overarching security strategy and oversight.

The key challenges were:

- Lack of technology service optimization across global sites
- Variable risk mitigation strategies across environments and business units
- Operational silos and lack of workflow integration
- Diverse and fragile technology environments
- Insufficient cybersecurity leadership and oversight

The Solutions

- Complete an enterprise level assessment using NIST (National Institute of Standards and Technology) Cyber Security Framework (CSF) to identify gaps and prioritize improvements
- Conduct penetration and vulnerability testing across all environments
- Create sustainable cybersecurity policies and operational standards
- Engage legal and human resources leaders to develop and enforce a consistent security awareness program
- Develop and deploy consistent controls for EDR (Endpoint Detection and Response)
- Implement consistent patch management and incident reporting practices
- Write job descriptions and participate in the selection process for technology leadership positions
- Optimize telecom services over a united VOIP (Voice Over IP) solution
- Centralize over 180 domains on a single domain management platform

The Results

The organization significantly improved several key areas by enhancing security and improving operational efficiency. Enterprise-wide penetration and vulnerability testing, which had never been done before, yielded new insights into assets, inconsistencies and deficiencies across environments. These results, together with the NIST CSF assessment, informed prioritizing vulnerability remediation, protection, and detection improvements. Consistency in endpoint detection and response was established and accompanied by a more robust security awareness program with explicit protocols that significantly improved the overall security posture.

The organization met expectations for cyber insurance by implementing mature controls that demonstrated Fortium's ability to keep pace with escalating industry standards. Critical security measures, such as multifactor authentication, were successfully adopted, and the organization developed a keen awareness for prioritizing spending and resource allocation effectively. Additionally, telephone and domain management improvements contributed to a comprehensive understanding of their current technology assets and cyber risk position.