fortium partners

Case Study

Overhauling Cybersecurity: How a Fortium CISO Helped a Healthcare Organization Thrive

Client Profile

- Healthcare company
- Annual Revenue: $85M
- ~200 employees
- HQ: Houston, TX

The Challenges

Before Fortium's engagement, a prominent healthcare organization faced significant operational disruptions, inefficiencies, and higher risks due to high turnover in its IT leadership. Two significant departures left the company vulnerable and in urgent need of a strategic and operational overhaul: the Chief Information Security Officer (CISO) and six months thereafter, the Director of IT. The organization's HR department struggled to recruit and interview qualified candidates in a timely way which resulted in a significant gap in IT service levels and high risks for cybersecurity vulnerabilities. Given the organization's status as a high-value target (HVT) for cybersecurity threats, there was an immediate need to quickly transition from a reactive to a proactive security posture, especially in the context of stringent healthcare regulations and compliance requirements.

Key Challenges:

- **High Turnover**: The sudden departure of the CISO and IT Director left a leadership vacuum and forced the remaining staff to take on fractional roles that were well beyond their expertise.
- **Critical Need for Scalable IT and Robust Cybersecurity:** As a high-value target (HVT) for cybersecurity threats, the organization urgently needed to rebuild its IT and cybersecurity teams and infrastructure.
- **Reactive Security Posture:** The organization was operating with significant gaps in its security measures and shifted its approach to be reactive rather than proactive, which resulted in an unsafe security framework.
- **Healthcare Compliance Requirements:** Achieving complex cybersecurity certifications, such as HITRUST, was particularly challenging, requiring 1.5 to 2 years of dedicated effort to meet regulatory demands without CISO expertise.

The Solutions

To address the critical challenges and mitigate risks, Fortium Partners' fractional CISO implemented the following strategies:

- **Hired a New Team:** Fortium brought in a new IT and security team to stabilize operations, address critical gaps, and get IT spend under control.
- **Completed a Comprehensive Assessment:** Identified significant vulnerabilities and gaps in the organization's IT and security infrastructure that enabled targeted improvements.
- **Strengthened EDR and Vulnerability Management:** Enhanced Endpoint Detection and Response (EDR) capabilities and established a proactive vulnerability management program to safeguard the organization.
- **Established Control Measures and Governance:** Introduced a Technology Management Committee and Architecture Review Board to govern technology procurement and reduce shadow IT risks.
- **Adapted to Rapid Organizational Changes:** Supported the organization's post-COVID contraction and positioned it for renewed growth with a focus on streamlined compliant processes and centralized systems.

The Results:

Fortium Partners' engagement led to a significant cultural shift toward accountability and control within the organization. By establishing control measures, including a Technology Management Committee and an Architecture Review Board, the company eliminated unregulated technology purchases and mitigated the risks associated with shadow IT (the use of technology or resources without the knowledge or approval of IT). Optimized management access and permissions also enhanced security and streamlined operational efficiencies. The organization now benefits from Fortium's strategic initiative and technology leadership, which results in a more robust technology governance and a foundation for sustainable growth and innovation.

972.827.8137 info@fortiumpartners.com fortiumpartners.com