protiviti®
Face the Future with Confidence

Avoiding the headlines: Healthcare organization commits to raising its cybersecurity competency to buck the industry norm

Keys to Success

CHANGE REQUESTED

Improve ability to deliver IT security functions to mitigate potential data breaches and other cybersecurity threats.

CHANGE ENVISIONED

Leverage strong executive and board support to build up the IT security department, institute a proactive cybersecurity culture, and emphasize cyber-threat awareness and management.

CHANGE ACHIEVED

Approximately 30 risk remediation and training projects strengthened the organization's cybersecurity posture and raised cyber-risk tolerance to a high level relative to the healthcare industry.

Over the last several years, the growing number of cyber attacks has exposed the lack of IT cyber defenses across all industries, but healthcare organizations have been perhaps the least prepared. This is made clear by the frequency, size and impact of healthcare breaches, and the fact that many of these breaches are revealed to have gone on for months before being discovered.

Recognizing these threats, a healthcare organization with significant hospital and physician group operations across the U.S. and globally reached out to Protiviti to assess its cybersecurity capabilities. The organization was achieving annualized growth of 20 percent through expansion and acquisitions, but it recognized that the increase in security demands that accompanied this growth was straining the IT department's ability to prevent cyber attacks. The last thing the organization wanted was to end up in the news as the next healthcare cybersecurity failure and wrestle with the subsequent financial, regulatory and public relations nightmare — so it engaged Protiviti to help.

Using leading industry standard ISO 27001/2, Protiviti conducted a three-month assessment that uncovered several significant cybersecurity weaknesses. At the root of these issues was an underfunded and understaffed IT security department that was operating in a reaction mode and had no time to assess threats proactively. That fueled doubt about the department's ability to protect digital assets and led to attrition among overburdened and demoralized IT security staffers. Measured by the Carnegie Mellon Capability Maturity Model (CMM), the organization's cybersecurity risk tolerance levels were well short of the healthcare industry average.

"Protiviti has been an extremely integral partner for our organization over the past years, both from a delivery and leadership perspective. Protiviti's knowledge and willingness to go above and beyond has far exceeded each of our team members' expectations."

— Chief Information Security Officer

The alarming picture that emerged from the assessment galvanized the healthcare organization's executive team and board of directors, who threw their support behind an ambitious Protiviti-designed program and training strategy to remediate weaknesses and mitigate threats. Aware that organizations are inherently resistant to change, executives committed to top-level sponsorship of the program to ensure its success.

The decision to hire a chief information security officer (CISO) in a newly created senior executive position underscored the client's dedication to strengthen the division, emphasize its importance and make it accountable. It was a commitment that was evident early on when company management asked a Protiviti team member to step in as interim CISO before a permanent CISO was hired.

Protiviti worked with the organization to initiate nearly 30 major tactical and strategic risk remediation projects, including implementation of several data protection technologies; mitigation of vulnerabilities across desktop computers, laptops, servers and other devices; enhancement of third-party risk management; and bolstering of database and identity management security. Protiviti's cybersecurity experts are continuing to provide ongoing vulnerability testing and are spearheading improvements in medical device security, among other current initiatives.

"Protiviti has been an extremely integral partner for our organization over the past years, both from a delivery and leadership perspective," said the company's CISO. "Protiviti's knowledge and willingness to go above and beyond has far exceeded each of our team members' expectations."

Training and Other Keys to Success

While many companies often find change "on the ground" difficult due to the ingrained habits of personnel, the organization's backing of employee training plans has played a pivotal role in the cybersecurity improvement program. Creating a meaningful message without being overbearing proved effective in helping the organization's personnel realize that changing behaviors and honing awareness were essential to protecting sensitive information and minimizing liability. Cybersecurity and cyber-awareness training included on-demand, web-based education of nurses, doctors and others about the dangers of clicking on potentially malicious links or providing credentials to unverified associations or organizations.

The enhanced cybersecurity capabilities of the IT security department and its proactive operating approach have earned it the confidence of its stakeholders in the organization, and staff attrition is at a minimum. Most impressively, the organization's CMM ranking has risen to a level that is now at the high end of the healthcare industry average.

An important success factor in this project was access to experienced resources to supplement IT security staffing needs. Some of those workers, placed through Protiviti's managed business services partner Robert Half, transitioned to become full-time employees of the organization. With the additional hiring, the department saw a roughly fourfold increase in staff, corresponding to the company's rapid growth in new markets.

These measures have strengthened the healthcare organization's cybersecurity posture substantially. The company now boasts robust remediation and mitigation capabilities and strong awareness of digital threats. Identity management risks have declined by 53 percent, and the ability to recognize phishing campaigns has more than doubled compared to 2015.

The enhanced cybersecurity capabilities of the IT security department and its proactive operating approach have earned it the confidence of its stakeholders in the organization, and staff attrition is at a minimum. Most impressively, the organization's CMM ranking has risen to a level that is now at the high end of the healthcare industry average. None of these advances would have been possible, however, without the client's executive-level drive and commitment to transform its IT security department from industry laggard to an industry leader.

protiviti®