protiviti®

Face the Future with Confidence

Healthcare Cybersecurity Services

Breaches and cyberattacks are on the rise in the healthcare industry and the reality is that lives are now at stake. The recent acceleration of digital technology and connectivity within healthcare has led to significant improvements in patient care delivery, more effective population health management and better patient outcomes. With this increased technology and connectivity, however, comes increased exposure to cyberattacks that can impact patient care delivery, safety and privacy. Many healthcare providers need additional, immediate improvements to address these new risks. Unfortunately, this new risk environment is also combined with an overall shortage of qualified security professionals, which means that healthcare providers, now more than ever, need a trusted partner they can team with to help achieve their goals of continually enhancing patient privacy and safety. Protiviti has made significant investments in thought leadership, methodology and personnel to be that partner.

Cybersecurity Transformation & Remediation Services

Creating and establishing an effective cybersecurity program in healthcare has numerous challenges and barriers, many unique to the industry. Typically, healthcare IT and security departments remain under-funded, go without sufficient skilled resources and lack key technologies. Protiviti:

- Works with healthcare providers to assess the current state of their capabilities, architect a future state of information security and develop roadmaps, identify the initiatives to achieve prioritized remediation goals, formally request funding to executive leadership, and deliver the initiatives to achieve your organization's cybersecurity vision.
- Helps technology and business leaders develop and implement an effective and proactive security approach that ties security to organizational goals, combats a widening array of threats, and embraces emerging technology to efficiently manage risk.
- Provides a smooth and efficient path to remediation through a wide range of ongoing services, such as policy and procedure development, security awareness training, security technology implementation, network and system control improvements, risk management program briefings and discussions, interim Chief Information Security Officer services, and cybersecurity staff augmentation.

Cybersecurity Framework Assessments & HITRUST Certification

Healthcare providers are being asked to demonstrate that they meet a variety of security and privacy requirements outlined by regulatory and industry frameworks such as the HIPAA Security, Privacy, and Breach Notification Rules; HITRUST CSF; NIST CSF; ISO 27001/2; and other standards. This can be an immense effort, especially for teams that have not gone through this process before. Protiviti:

- Assists in assessing, improving and sustaining the maturity of security programs against these frameworks within healthcare providers through experts with significant experience with the frameworks and related regulations.
- Facilitates certification with the HITRUST CSF through initial gap assessments, remediation assistance, and final certification submission as a designated HITRUST CSF Assessor.
- Helps refine or design framework-supporting security controls that are not overly intrusive to the employee and do not impede business operations or inspire avoidance.

HIPAA Security Risk Analysis

HIPAA requires that organizations perform security risk analyses across the full scope of the ePHI within their environment through a structured and robust program. Many organizations struggle to identify all instances of ePHI as well as to perform holistic risk assessments in an efficient manner. Protiviti:

- Helps identify where ePHI resides and reveals meaningful insight into key risks as well as facilitates HIPAA compliance.
- Ensures a smooth and efficient risk analysis through a proven methodology and experts with deep healthcare business, technology and information security experience.
- Enables effective control remediation through recommending risk management activities that have proven to be successful in other healthcare environments.

Medical Device Security

Medical device security has gained attention as more vulnerabilities have been identified by healthcare providers and security researchers that could result in physical harm and even death of the patient relying on these critical devices. Ransomware outbreaks have shown that these devices can be accidentally impacted by broader attacks. While many leading device manufacturers have made security improvements in new devices, there are still many legacy medical devices as well as devices from less security-aware manufacturers that introduce risk to patient safety. Protiviti:

- Helps assess and communicate the potential risk and impact of medical device security through a holistic process and technology assessment of the entire lifecycle of a medical device.
- Assists in developing a remediation roadmap and provides specific recommendations for remediating medical device security issues.
- Reduces the risk to patient safety by implementing network segmentation, developing device hardening standards, designing effective device lifecycle management methodologies, and implementing other key controls.

Vulnerability Assessment & Penetration Testing

The healthcare industry is a prime target for nefarious parties to exploit security weaknesses and gain access to data rich with sensitive information that can then be sold in underground markets for a premium. It is important that healthcare providers routinely evaluate their security controls through realistic testing to find flaws before attackers do. Protiviti:

- Utilizes fully functional state-of-the-art security labs across the country, helps assess exposures on Internet-facing systems as well as those present on the internal network, and employs highly experienced and qualified teams of practitioners specialized in technical security assessments.
- Identifies unpatched vulnerabilities and determines the root cause of existing vulnerabilities in your

environment through assessing applications, web-based systems, medical devices, databases and other connected systems.

- Facilitates remediation of vulnerabilities through detailed remediation recommendations and the provision of supporting services such as control improvement projects and security awareness training.

Vendor Risk Management

Healthcare providers utilize numerous third-party vendors to provide specialized services aimed at enabling the most effective and efficient care delivery process. While these third parties are expected to use the same level of scrutiny to protect sensitive information, trends have shown that these same vendors are a leading point of breaches of sensitive information, resulting in potential reputational and financial risk for the healthcare provider that engaged them. Protiviti:

- Helps mitigate vendor risk through the development and implementation of mature vendor risk management programs (that cover the full lifecycle, from evaluation through termination).
- Enables efficient vendor assessments through the outsourced performance of technology-facilitated vendor assessments, either remote or on-site.

PCI Compliance

Healthcare providers must protect payment card data along with their PHI. PCI compliance requirements are often difficult to interpret and very expensive if not strategically implemented. Protiviti:

- Reveals the true risk to cardholder data through comprehensive PCI gap assessments by experienced, certified Qualified Security Assessors that have performed many final Reports on Compliance.
- Enables a sustainable and cost-effective process for ongoing compliance from the evaluation of key strategies such as point-to-point encryption and payment page outsourcing to remediation support and the final assessment.

Healthcare Cybersecurity Transformation — Case Study

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

Project Objective

Protiviti's client is an international, not-for-profit healthcare provider that operates over 60 hospitals and 350 clinics in four countries. The client was experiencing 20% annualized growth through expansion and acquisitions. This organization's growth and other high-priority business demands had negative consequences on their Information Security organization, including: excessive resource attrition, significant loss of confidence by the business leaders in the ability to protect the organization's digital assets, numerous unplanned technology failures and poor perceived delivery quality by the business. Based upon a long-standing relationship with this client, Protiviti built and co-delivered a cybersecurity program to mitigate risk and improve quality of delivery. Common project objectives include:

- Design and deliver annual cybersecurity strategy and program
- Mitigate active and emerging threats and exposures
- Demonstrable and quantifiable cybersecurity risk reduction
- Business and executive objectives alignment
- Predictable security budgeting

Protiviti Approach

In late 2014, Protiviti began supporting the client by performing a capability maturity assessment based upon a leading industry standard (ISO 27001/2) to understand their current risks and exposures. This assessment identified numerous significant cybersecurity risks, exposures and technology limitations that were well beyond a typical healthcare organization's risk tolerance levels. As a follow-up to identifying the risk mitigation gaps, Protiviti partnered with the client to build and co-deliver a three-year strategic cybersecurity program. With the client's oversight and direction, Protiviti spearheaded several major security projects, including: discovery of sensitive data, implementation of several data protection technologies (e.g., cloud data security, host-based DLP, etc.), security awareness training, vulnerability management, system security hardening, cyber incident response, privileged user account risk mitigation and modernization, access provisioning/certification management, and a formal document management program to establish approved and actionable cyber security policies, procedures and standards. In addition to the 20 major projects (80,000 hours effort) that Protiviti has delivered over the past three years, Protiviti provided temporary loan staff to fill active security operational needs and has plans to deliver 10 additional security projects (40,000 hours effort) to take the client to the next level of cybersecurity program maturity.

Benefits Achieved

Our sustained presence with this Healthcare client has resulted in significant improvements in their cybersecurity capabilities, risk mitigation to acceptable risk tolerance levels and significant improvement within their program maturity. The Identity and Access management initiative resulted in a 53% reduction in superfluous Active Directory (AD) groups and the standardization of AD management toolkits. Over the past three years, the security awareness training program has reduced phishing campaign testing click-through and compromise failures by half, from 15% in 2015 to 7% in 2017. Protiviti loan staff have supplemented the Information Security team by 30% and reduced risk indicators by an average of 80%.

Contacts

Richard Williams
Managing Director
Global Healthcare Industry Lead
+1.214.395.1662
richard.williams@protiviti.com

Matthew Jackson
Managing Director
Healthcare IT Solutions Lead
+1.214.284.3588
matthew.jackson@protiviti.com