Case Study

Medical Center Restores Regulatory Compliance and Resets Security Strategy

The client

The client is an independent, award-winning medical center located in the West. Established more than 100 years ago, the multibillion-dollar hospital has earned national recognition for pioneering leading-edge treatments and procedures, serving thousands of patients every year with groundbreaking technology and lifesaving care.

The challenge: Resolve snowballing compliance issues and establish a well-managed information security program

Medical centers have a critical responsibility to protect patient privacy under the Health Insurance Portability and Accountability Act (HIPAA). Despite efforts to implement HITRUST standards — a certifiable control framework that encompasses HIPAA, Federal Trade Commission (FTC), and other data security regulations — the client's number of outstanding security audit findings left unaddressed had recently surpassed 300.

Protecting the center's valuable intellectual capital was also an important task left largely unattended. As a nationally recognized facility with valuable contributions to medical research, they face the ongoing risk of intellectual property theft.

Their goal was to establish an effective Information Security Management Program (ISMP), but they had significant personnel challenges, including an unexpected vacancy for the position of Chief Information Security Officer (CISO) and no security architect.

Industry:

Healthcare

Insight provided:

- Consulting and collaboration with client's executive leadership
- Security environment assessments (HITRUST, PCI-DSS, risk mitigation)
- On-site technical resources and project management
- Design and implementation of an industry standard ISMP
- Ongoing support for security program improvements

Insight services:

- Consulting Services
- Security Strategy Workshop
- Virtual Chief Information Security Officer (vCISO)

The solution: Executive-level, on-site security services and expert strategic guidance

Meeting the client's needs first required identifying security system weaknesses and building a roadmap to address them. Without a CISO to guide the process, the most effective solution involved supplementing their security team leadership through our Virtual Chief Information Security Officer (vCISO) program.

The newly designated vCISO joined the client's information security program team on-site to assess their entire security environment. All unaddressed security findings were prioritized by risk level, and individual corrective action plans were developed and executed to enable the client to meet HITRUST standards. When the client found and placed a qualified, permanent CISO, the Insight team continued to support the client in a reorganization of their IT and security organization, which eventually will move the CISO out from under the CIO and reporting directly to the compliance officer.

During our assessments, we discovered the client was out of compliance with Payment Card Industry Data Security Standards (PCI-DSS). We performed a PCI-DSS assessment and helped them regain compliance, plus introduce new technology and procedures to consolidate their payment card agreements and better protect financial information.

With high-risk compliance and security concerns mitigated, we shifted focus toward a comprehensive ISMP by:

- Identifying interdepartmental issues
- Defining a security control framework
- Establishing well-defined roles within departments
- Educating all stakeholders, up to the Board of Directors

Plans have been developed and approved for implementing further security improvements, including technology and process changes.

The benefits: Improved information protection and compliance and a stronger security posture

Through our vCISO program, the client was able to quickly fill knowledge and bandwidth gaps in their security team to mitigate noncompliance risks, improve protection of patient information, successfully pass audits, and work toward building a robust security program. When the client placed a new, permanent CISO, the vCISO and his team helped onboard and train the new CISO for a smooth transition.

Since the start of our engagement, the medical center has been audited several times but has received no further findings from the Office of Civil Rights. The client's security team is now freer to focus on strategic initiatives in progress, including replacing legacy systems and pursuing cross-organizational security developments.

Today, the client enjoys improved access management, better clarity around organizational roles and responsibilities, and a comprehensive approach to security that is amenable to enhancements. For instance, the Insight team is now working with the client to include medical devices in the scope of information security management, extending their security program all the way to the edge. As the hospital continues to succeed as a research leader and care provider, having a secure foundation will be invaluable.

Benefits:

- Regulatory compliance and penalty avoidance
- A well-defined ISMP
- Improved organizational structure to promote security and compliance
- Increased awareness and buy-in to security initiatives across hospital teams
- Better access management and visibility across the security environment
- Freed internal resources for other hospital security initiatives