CASE STUDY

Virtual Chief Information Security Officers for Healthcare

Fractional leadership with cybersecurity expertise offers new hope to security healthcare leaders and organizations without a dedicated CISO.

THE CLIENT

An organization was concerned that their cybersecurity posture posed significant risk to their growth agenda, revenue goals, and patient outcome standards. Resources were always scarce – even for top priorities, they decided to engage a Chief Informational Security Officer (CISO) on a fractional basis. *Why?* This approach made the most practical and financial sense because 1.) it fit within their budget constraints and 2.) cybersecurity risks necessitated expert involvement.

CHALLENGE

The organization had designated several teams to participate in cybersecurity efforts: Security Council, Steering Team, IT Security Committee, and appointed a Security Officer. However, each individual was assigned this role in addition to their existing leadership responsibilities. The organization needed to extend the expertise of their leadership team without incurring the budget of an additional executive.

> Healthcare leaders know about gaps in their cybersecurity programs. They need extra hands to prioritize what needs to be done and to scope the effort without impeding the progress of competing priorities.

Ryan Finlay
Principal CISO | *CereCore*

Editor's note: *For their protection, CereCore keeps the identities of cybersecurity clients confidential.*

p: 855.276.9112 | **e:** info@cerecore.net

HOW WE HELPED

A virtual Chief Information Security Officer (vCISO) from CereCore fortified the cybersecurity program with specialized expertise and healthcare focus, all while delivering significant savings and efficiency gains as compared to recruiting a full-time executive leader for the organization.

The vCISO worked as an advisor for the assigned security officer under HIPAA regulations. The security officer manages the security program, leveraging the advice and counsel of the vCISO. The vCISO provided strategic direction, expertise, and capacity to enhance the organization's security program. *The vCISO assisted this organization in three areas:*

1. **Defining the cybersecurity strategy**
2. **Building cybersecurity resilience**
3. **Improving cybersecurity posture** *(defense against risks and vulnerabilities)*

1 Defining the cybersecurity strategy.

The strategy was based on:

- Current threats and risks relevant to the organization
- Compliance requirements
- Business and IT requirements

An assessment of the current security program was conducted, including cyber resilience, and priorities were determined by the security governance committee and the vCISO.
Understanding of the NIST cybersecurity framework informed a targeted security framework focused on functions to identify, protect, detect, respond, and recover from cybersecurity threats and risks.

VCISO SUPPORT IN THE EVENT OF A BREACH?

Thankfully, no breach was experienced by this client, but the vCISO would have provided guidance and leadership in the event of a serious cyber breach. The vCISO's prior experience with response approaches, expertise in healthcare's threat landscape, and familiarity with the organization would prove to be invaluable, potentially saving significant costs and downtime associated with breach recovery.

2 Building cybersecurity resilience.

Cyber resilience is an organization's ability to continue delivering services despite adverse cyber events. The vCISO evaluated the organization's current state and provided regulatory compliant recommendations to avoid, respond and recover from events.

3 Improved cybersecurity posture.

The vCISO studied the organization's current security operations including these processes/workflows:

- Identity and access management
- Security monitoring and response
- Threat and vulnerability management
- Configuration management
- Asset management
- Security awareness training
- Risk assessment and risk management

The vCISO maintained a comprehensive understanding of threats to the healthcare organization by monitoring sources including: InfraGard, Cybersecurity Infrastructure Security Agency (CISA), US-CERT, US Department of Health and Human Services (HHS) and others.

cerecore®
cerecore.net
p: 855.276.9112 | **e:** info@cerecore.net

CereCore® provides IT services that make it easier for you to focus on supporting hospital operations and transforming healthcare through technology. With a heritage rooted in our nation's top-performing hospitals, we serve as leaders and experts in technology, operations, data security, and clinical applications. We partner with clients to become an extension of the team through comprehensive IT and application support, technical professional and managed services, IT advisory services, and EHR consulting, because we know firsthand the power that integrated technology has on patient care and communities.